UNIVERSITY OF CALIFORNIA

Los Angeles

Facing the Faceless Adversaries:
Criminal Deterrence Theory, Informal Sanctions, and Status-Seeking Motives in Explaining Why Bare Indictments Deter Cyberattacks

A dissertation submitted in partial satisfaction of the

requirements for the degree Doctor of Philosophy

in Political Science

by

Melissa Quynh-Tien Nguyen

2022

ABSTRACT OF THE DISSERTATION

Facing the Faceless Adversaries:

Criminal Deterrence Theory, Informal Sanctions, and Status-Seeking Motives

in Explaining Why Bare Indictments Deter Cyberattacks

by

Melissa Quynh-Tien Nguyen

Doctor of Philosophy in Political Science

University of California, Los Angeles, 2022

Professor Michael S.Y. Chwe, Chair

Since 2014, the U.S. has pursuant to 18 U.S.C. § 1030 issued and publicized federal criminal indictments against nation-state cyber adversaries. Because these "bare" indictments are issued against foreign nationals from jurisdictions that are not party to a bilateral extradition treaty with the U.S., it is seen as highly unlikely that these indicted foreign nationals will ever face trial, much less be convicted. Data suggests that bare indictments may have contributed to deterrence – persuading cyber adversaries that the costs of mounting cyberattacks will outweigh the benefits – but causality has not been rigorously proven; furthermore, the reasons why bare indictments can deter cyberattacks remain unexplained. Drawing from the principles of criminal deterrence theory and its associated literature on informal sanctions, this dissertation project utilizes behavioral analysis of

motive within a case study approach to demonstrate that bare indictments' labeling the alleged cyberattacker a 'criminal outcast' can achieve deterrence. This project theorizes and finds that the informal sanctions triggered by the issuance and publicization of bare indictments tend to directly deny the objectives of status-seeking cyber adversaries and indirectly outweigh the aims of thrill-seeking cyber adversaries, but tend not to deter profit-seeking cyber adversaries. Moreover, the project engages with attribution theory to show that making the issuance of a bare indictment common knowledge serves as an attack on nation-state status in the international community. The case studies – spanning China, North Korea, Iran, and Russia – serve as the basis for in-depth policy recommendations. In providing suggestions for optimal leverage of bare indictments as a deterrent measure, this project argues that future threats such as cyber warfare and hybrid warfare may be countered by using domestic criminal law as an efficient means of unilateral norm formation amongst the global order.

Keywords: attack to face, attribution theory, criminal deterrence theory, criminal motive, cyberattacks, cyber deterrence, cyber war, cyber warfare, data theft, DDoS, hybrid war, hybrid warfare, informal sanctions, prestige, *respondeat superior*, status

The dissertation of Melissa Quynh-Tien Nguyen is approved.

Eric Aram Min

Richard H. Sander

Robert Trager

Michael S.Y. Chwe, Committee Chair

University of California, Los Angeles

2022

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

The content of this dissertation, “Facing the Faceless Adversaries,” does not constitute legal advice.

No disparagement of any legal person is intended.

Legal protection of the statements made in this dissertation is likely enforceable pursuant to California Code of Civil Procedure § 425.16.(e)(3) as well as under other applicable law.

M.Q.T.N.

June 2022

VITA

Melissa Q.T. Nguyen is an American lawyer and political scientist whose interdisciplinary research examines the interactions among ethics, morality, law, and policy in shaping individual, organizational, entity, and state behavior. Having been a dual degree candidate at the UCLA School of Law and the UCLA Department of Political Science, Ms. Nguyen holds a J.D. with a specialization in Business Law and Policy, emphasis in Taxation. During her time at UCLA Law, Ms. Nguyen was a Dean's Merit Scholar, and she served as speakership project lead on organizing the first academic event ever to be jointly hosted by UCLA Law and UCLA Political Science. Her M.A. work refuted the argument that Jeremy Bentham's utilitarian deterrence theory allows for punishing the innocent.

Ms. Nguyen has held research fellowships from UCLA Law's Promise Institute for Human Rights and from UCLA's Bedari Kindness Institute. As a graduating junior in the UCLA College Honors Program, Ms. Nguyen received her B.A. in Political Science *magna cum laude* and was inducted into Phi Beta Kappa membership; subsequently, she was accorded a Phi Beta Kappa Graduate Study Award. She graduated as a valedictorian of Pacific Coast High School, a hybrid in-person and online independent study program based in Orange County, California. Prior to commencing her postgraduate studies, Ms. Nguyen was professionally active as a classical pianist and accolade-winning composer who concertized in solo, chamber, and symphonic settings.

CHAPTER 1

INTRODUCTION: A CRIMINAL DETERRENCE THEORY FOR A GLOBAL FUTURE

On May 19, 2014, the United States Department of Justice's Office of Public Affairs released a press statement announcing that a federal criminal indictment had been issued against five military officers of the Chinese People's Liberation Army for thirty-one counts of crimes relating to economic espionage carried out by means of unauthorized access to computerized systems (U.S. Department of Justice: Office of Public Affairs, May 19, 2014). Although the relevant federal statutory law – 18 U.S.C. § 1030 – had been enacted three decades prior, this indictment was characterized as a novel enforcement of this domestic law against international state actors. In U.S. Attorney General Eric Holder's words, which were in turn highlighted by news outlets (Nakashima and Wan 2014; BBC News 2014), the indictment "[represented] the first ever charges against a state actor" – namely, China – "for this type of hacking" (U.S. Department of Justice: Office of Public Affairs, May 19, 2014).

The verbal response made on behalf of China arrived swiftly and indignantly. In remarks circulated globally on May 20, Spokesperson Qin Gang of the Chinese Foreign Ministry called the U.S.'s enforcement of 18 U.S.C. § 1030 against China improper, a "[gross violation of] the basic norms governing international relations" (Qin 2014). Moreover, Qin asserted that the criminal indictment itself was invalid in having been "based on deliberately fabricated facts" (Qin 2014). Qin further criticized the U.S.'s actions as diplomatically unsound with respect to foreign relations, saying that the indictment "jeopardizes U.S.-China cooperation" (Qin 2014).

One year later, however, a cooperative milestone on cybersecurity matters was reached by the respective heads of state of the two nations. In September 2015, U.S. President Barack Obama and Chinese President Xi Jinping arrived at an agreement that was committed to writing by and immediately released via the U.S. White House's Office of the Press Secretary (White House 2015). Interestingly, and in contrast to Qin's dire prediction of undermined relations between the U.S. and China, the written text of Obama's and Xi's September 2015 agreement expressly invoked cooperation. The first of four provisions on cybersecurity reads in part, "both sides agree to cooperate… with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory" (White House 2015). The second, which has been the focus of much analysis and debate (Harold 2016; Farley 2018; Lin 2018), constrained each party's own conduct not only toward the other nation, but toward the entire world. Under the second provision of the agreement, neither the U.S. nor China would condone hacking if the purpose were to steal information to be used for private profit, irrespective of the target of such hacking: "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property… with the intent of providing competitive advantages to companies or commercial sectors" (White House 2015). The agreement also addressed international norms, as the third of the cybersecurity provisions begins, "Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community" (White House 2015).

Since May 2014's first instance of indicting alleged nation-state actors for malicious cyber activity, the U.S. has gone on to indict many other putative nation-state actors for the commission of cyber-enabled criminal offenses. The U.S. has issued these federal

indictments not only against more Chinese individuals (*Su Bin* indictment), but also against individuals from Russia (*Dokuchaev* indictment), Iran (*Fathi* indictment), or North Korea (*Jon* indictment). Although scholars have observed this phenomenon and characterized as a *de facto* policy the U.S.'s indictments of putative nation-state actors for cyber offenses (Wilner 2020, 264; Keitner 2019, 207), much remains unexplained about the above Chinese case, and about the efficacy of the U.S.'s policy in practice.

Basic principles of American federal criminal procedure might indicate that the indictment of the five People's Liberation Army officers unfolded against a background of seeming pointlessness. Under U.S. law, the formal punishment for committing a crime cannot be imposed unless the individual is convicted; for the accused individual to be convicted, the accused individual must have either faced a legal trial, or waived trial and pled guilty to the crime. Because China has no extradition treaty with the U.S. to compel China's sending indicted individuals to face trial in a U.S. court of law, it would have been evident to both the U.S. and China that it was highly unlikely that the Chinese military officers would be tried – much less convicted – as a result of the indictment. Moreover, China's laws – like the laws of many other national jurisdictions – prohibit the nation from extraditing the nation's own nationals. Considering the apparent improbability that the indicted individuals would 'voluntarily' choose to come to the U.S. and face trial, China could have expected with almost total certainty that the formal punishment for violating 18 U.S.C. § 1030 would never be imposed upon its indicted officers. Indictments such as these can be termed *bare indictments*; since these criminal charges are issued against foreign nationals from a nation that does not have an extradition treaty with the U.S., these

criminal charges are arguably unlikely to result in enforcement of the formal punishment for the crime.

This information generates some puzzling questions. If it was obvious from the outset that the U.S. indictment of the Chinese military officers would probably not amount to anything more than a 'bare' indictment, why did China see fit to respond at all to the U.S. indictment? If basic legal principles dictate that bare indictments are unlikely to lead to the imposition of formal criminal punishment, why would U.S. authorities continue the *de facto* policy of issuing bare indictments?

Another sweeping question generated by this case and the phenomenon of "attribution by indictment" (Keitner 2019, 207) resonates with the ongoing scholarly debate over how *deterrence* –preventing an adversary from taking an action by convincing the adversary that the costs of that action will outweigh the benefits (see George and Smoke 1974, 11) – may be achieved in the cyber arena. If a criminal indictment did indeed achieve a deterrent effect in the May 2014 Chinese case, what insights does the case reveal about nations' ability to leverage indictments and associated tools of domestic criminal law in order to prevent future cyberattacks?

This dissertation project draws upon principles of *criminal deterrence theory* ("CDT") – a branch of deterrence that aims to prevent crime and spans across many disciplines including economics, behavioral psychology, legal philosophy, sociology, and criminology – to explain why bare indictments deter cyberattacks. Bare indictments label the target a 'criminal outcast.' Through this labeling mechanism, bare indictments achieve a deterrent effect by triggering a package of *informal sanctions* against the target of the indictment. These informal sanctions include practical, emotional, and social negative

consequences. Extrapolating from criminological studies on the motivations of cyberattackers and sociological studies on the deterrent effect of informal sanctions, I theorize that bare indictments are likely to deter actors with primarily thrill-seeking or status-seeking motives for mounting cyberattacks. By contrast, bare indictments are unlikely to deter actors with primarily profit-seeking motives for mounting cyberattacks. The informal sanctions triggered by bare indictments can serve as an *attack on face* that directly frustrates status-seeking aims, with status-seeking – the desire to attain or maintain a relatively high rank in a social hierarchy, an objective that can be accomplished by acquiring markers of prestige – being a frequent motive among state-sponsored cyberattackers. Furthermore, bare indictments frustrate status-seeking because the label of "criminal outcast" is inherently incompatible with nation-state objectives of holding a high rank in the social hierarchy of the international community. Bare indictments countervail thrill-seeking because the practical consequences of a bare indictment are frequently sufficient to outweigh the emotional thrill of mounting a cyberattack. The trigger of informal sanctions accomplished by labeling the alleged cyberattacker as a criminal outcast means that the issuance of bare indictments against specific cyberattackers can achieve a widespread deterrent effect among future potential cyberattackers by making their expected weighted cost outweigh their expected weighted benefit in the cost-benefit calculus.

I test this theory against case studies involving bare indictments issued by the U.S. against foreign actors who have allegedly committed cyberattacks. Nation-state cyberattackers could be thought to be far more challenging to deter than are nonstate cyberattackers, as nation-state actors who commit cyberattacks can be conceptualized as

having significantly greater resources and therefore much greater resolve than do nonstate cyberattackers (Libicki 2009, Bossler 2019). This analysis' findings are in accordance with the predictions of the theory. For example, China initially demonstrated primarily status-seeking motives for mounting cyberattacks. Accordingly, the data show that bare indictments issued against Chinese nation-state actors have arguably been highly effective deterrents against status-seeking cyberattacks. Meanwhile, North Korea has demonstrated primarily profit-seeking motives for mounting cyberattacks, and a bare indictment issued against North Korean nation-state actors has failed to deter future cyberattacks committed by the very same North Korean nation-state actors.

My theory on bare indictments hinges upon a principle from *attribution theory* – a psychological field of study examining what factors people assess to assign responsibility, culpability, and blame for actions (Fincham and Jaspars 1980). Attribution theory predicts that a perception of poor regard stemming from a state-sponsored actor's behavior is imputed to the nation-state under whose oversight that behavior was conducted.

Thus, although many of the case studies regard bare indictments of putative nation-state actors – where there is evidence to indicate that the nation-state from which the actor hails has directly benefited from the cyberattack – I hypothesize and find that bare indictments can deter at the nation-state level even when the bare indictments are issued against non-state rather than state actors. As is demonstrated most clearly by a case study involving the Russian state's preemptively taking action against its own nationals, bare indictments' attack on an indicted individual's status can be imputed to represent an attack on the status of the nation-state. Bare indictments apply a label of criminality, which is conceptually incompatible with holding a high rank in the global order. Much research in

international relations has shown that nation-states frequently hold objectives pertaining to status and prestige; bare indictments put those state objectives at risk, hence deterring cyberattacks at the nation-state level.

Since the general and specific deterrent effects that bare indictments achieve via attribution theory hinge on unfavorable perception by others as well as on the indicted actors' concerns over unfavorable perception by others in the social hierarchy of the international community, I construct this project's case studies by analyzing press statements, publicly released news reports, and other publicly available information. I use these case studies to offer in-depth recommendations for policy practitioners.

The government's crucial role in administering the criminal law to protect its citizens from falling victim to harmful offenses connects to how the bare indictment mechanism may be efficiently leveraged as a matter of policy practice. I show that the eighteenth-century theorists of CDT, classical criminologists (West 2017) Cesare Beccaria and Jeremy Bentham, each conceptualized criminal deterrence by means of criminal law as an essential constitutive function of the state. The criminal law itself can be considered a codified set of social norms, a catalogue of behavior that from the standpoint of that society is considered deviant and hence unacceptable (Bénabou and Tirole 2011, 17). As such, each issuance of criminal charges serves as a communicative reaffirmation, on the part of the issuing state, of what it considers to be its social norms. This norm-affirming function of the bare indictment leads to two reasons why it remains important to issue indictments even when it is likely that bare indictments will fail to deter the particular cyber adversary against which they are issued.

First, since the indictment is a communicative act, it serves as a means of unilateral norm-setting for general deterrent purposes. Each instance of formally labeling criminal behavior is another illustrative example, directed toward the general class of potential offenders, of what is considered to be unacceptable. The capability for the issuing state to set norms unilaterally, as opposed to necessarily requiring bilateral or multilateral agreement from other states, can serve as a powerful tool. As seen with the bare indictments issued by the U.S., imposing informal sanctions after-the-fact can delineate norms of conduct in the international order.

Second, as the administration of the criminal law is a crucial constitutive part of what defines a state, the issuance of indictments can serve as a symbolic reaffirmation of state sovereignty. It should be noted that the applicability of the international relations concept of *extended deterrence* – achieving deterrence on behalf of allies (Mazarr 2021, 15) – is limited here. The constraint of jurisdictional requisites means that one state usually cannot issue an indictment for crimes committed in another state. However, the investigative work required to support an indictment by determining the perpetrator of a cyberattack can be carried out by international allies and supporters, whether state or nonstate. These matters suggest that a state whose sovereignty is under threat – such as Ukraine, considering that Russia's February 2022 invasion of Ukraine is a conflict ongoing as of the time of this writing – can turn to allies for investigative support in enabling the state to issue domestic criminal indictments after-the-fact. The issuance of criminal indictments signals that the state is administering the protective function that makes it a sovereign state, and reaffirms the state's domestic norms before a global audience.

Given these effects, a counterintuitive finding of this project is that bare indictments may be a relatively more cost-efficient deterrent measure than are formal punishments. The improbability that a formal punishment will ever be borne by the accused foreign national of a non-extradition country has frequently been framed as a negative aspect of bare indictments, and deployed as a premise to support the contention that bare indictments cannot deter cyberattacks (see Goldsmith 2014; Lucas 2019; Pruitt 2021; Dugas 2021). If – as this project seeks to establish – bare indictments can and do achieve a significant deterrent effect on cyberattacks, then the improbability that the accused will come to face trial becomes a boon: when a state issues bare indictments, the state can deter cyberattacks without incurring expenses related to prosecution and trial. In other words, since it is highly unlikely that the targets of the indictment will 'call the bluff' of the issuing state, the state never has to 'follow through' with putting up the costs of securing a conviction or enforcing a formal punishment. Lest the state's capacity to use bare indictments as a 'bluff' appear to condone fabrication of charges or denial of the rights of the accused, I will show that CDT as well as criminal procedure provide ethical and practical safeguards against meritless indictments and restrain the issuing state from being unprepared to follow through. Thus, the issuance of bare indictments against cyberattacks holds much promise for further leverage as an efficient and ethically sound strategic policy.

Heretofore, scholars of cyber deterrence have almost exclusively focused on applying insights, principles, and models from what I term *state deterrence theory* ("SDT") – the branch of deterrence that deals with deterring state actors or state-like actors. Application of CDT principles harmonizes with application of SDT principles, yet CDT models provide added advantages. For example, as with how almost any actor – even a

private individual – can be a cyberattacker, CDT assumes that almost anyone can be a potential offender; virtually anyone, whether a member of that society or someone foreign to it, is capable of committing an offense that has been codified as a crime. The multitudinous composition of the class of potential offenders has resurfaced as a seemingly novel theoretical hindrance to cyber deterrence (Libicki 2009). Yet, from its earliest iterations, CDT has engaged with studying, formulating, and assessing solutions for this conceptual hurdle (Beccaria 1764b, 24; Bentham [1789] 1823, 24-25). One of these solutions is that which lies at the center of this study: the deployment of informal sanctions (Jacobs et al. 2000).

Identifying the mechanistic role of informal sanctions in driving bare indictments' deterrent effect upon cyberattacks not only speaks to optimizing bare indictments' continued use as a matter of strategic policy, but also makes a cross-disciplinary contribution to the literature. The field of cybersecurity usually presents *technical attribution*, or determining the perpetrator of a cyberattack, as a critical step for achieving deterrence in cybersecurity studies (Jensen 2012, 786; Healey 2011); this project examines how indictments efficiently mobilize the results of the technical attribution process into actualized deterrent effects. Informal sanctions, a concept studied in criminology and sociology, resonate with the branches of international relations known as *the English School* and *constructivism*, which focus on how social norms shape behaviors and influence interactions among members of the international community (Bellamy 2007). Understanding bare indictments indicates how individual members of the international community can leverage domestic criminal law to achieve unilateral norm-setting on the world stage. Thus, this project also serves as an example of how CDT principles may be

jointly leveraged with SDT principles to achieve and maximize deterrent effects, particularly with the onset of *hybrid warfare* that melds domestic criminality with interstate conflict.

The game of criminal deterrence is one simultaneously played against countless anonymous – "faceless" – adversaries. This model is particularly apposite in a world wherein cyberattacks transcend national borders and geographic distance, and when almost anyone – whether a private individual (Walsh 2021) or a nation-state entity (*Fathi* indictment) – can be a cyberattacker. Through formally attributing a cyberattack and labeling its alleged perpetrator a criminal outcast, the informal sanctions triggered by bare indictments engender forward-looking deterrence of future attempted harms. On a virtual battlefield where the desire for high regard – for what could be termed status, prestige, or "face" (Ho 1976) – is so frequently the motivating force for nation-state and non-state cyberattackers alike, bare indictments formally attribute cyberattacks to their anonymous perpetrators and label those cyberattackers criminal outcasts, serving as an attack to face that denies them their status-seeking objectives. Successfully facing the faceless adversaries, therefore, is accomplished by first revealing their faces and then stopping them from attaining the face that they seek.

The remainder of this dissertation project is organized as follows.

Chapter 2 provides a foundation for the theory by explaining necessary concepts from deterrence studies, criminology, criminal law, attribution theory, and international relations. Chapter 3 integrates these conceptual building blocks into a theory that positions the deterrent effect of criminal indictments as a trigger of informal sanctions. By

labeling the offender a 'criminal outcast,' informal sanctions directly deny the objectives of prestige-seeking cyberattackers and indirectly outweigh the aims of thrill-seeking cyberattackers. Chapter 3 also covers study design and data cleaning.

To prove the hypotheses raised in Chapter 3, Chapter 4 examines case studies regarding China, North Korea, and Iran. Providing context for the China cases, Section 4.1. analyzes the primacy of prestige in China's foreign policy. The primary case, covered in Section 4.2., concerns the U.S.'s 2014 indictment of five Chinese army officers for cyberattacks. By labeling the Chinese state a criminal outcast, bare indictments deterred China by directly frustrating its primarily prestige-seeking motives for allegedly mounting state-sponsored cyberattacks. Section 4.3. explains why the profit-seeking motives of North Korean actors make them undeterred by bare indictment. Rounding out the three common motives of cyberattackers, Section 4.4. shows that a bare indictment brought a campaign of thrill-seeking cyberattacks to an abrupt halt. Section 4.5. analyzes a large-scale trend from prestige-seeking to profit-seeking motives in Chinese cyberattacking activity, evidencing a norm-setting deterrent effect. Likewise, Section 4.6. discusses a similar trend toward profit-seeking among indicted Iranian cyberattackers. Section 4.7. analyzes the actions of an international coalition to explore the distinction between accusations of criminal misconduct and accusations of civil misconduct.

To show that the deterrent effects stemming from a bare indictment's accusation of criminality can be imputable against the state, Chapter 5 focuses on Russian case studies. In this chapter, I call attention to the high number of apprehended and convicted Russian non-state actors who were subject to bare indictment. I argue that the case of a convicted Russian non-state actor who was apprehended in a non-extradition country and the case of

Russia's cooperation with arresting a suspected non-state Russian cyberattacker show that – as attribution theory predicts – the Russian state does view bare indictments as attacks on its national status. This suggests a way that bare indictments may be used, going forward, to achieve a deterrent effect against nation-states themselves.

Chapter 6 focuses on counterexamples – cases in which the deterrent result is contrary to the predictions of the theory – to examine other aspects of bare indictments. Discussing what the Iranian state conceives of as markers of prestige, Section 6.1. provides context for the two counterexample cases. Next, the case study in Section 6.2. shows that a reason that lends bare indictments deterrent force is that they do not necessarily remain "bare"; bare indictments have led to apprehensions. Section 6.3. responds to some scholars' arguments that economic sanctions should always be imposed in tandem with bare indictments; the case study covered in this subsection serves as the basis for arguing that imposing economic sanctions can counterproductively undermine the deterrent effect of bare indictments.

Chapter 7 gives various implications for policy and in-depth recommendations for practitioners. Furthermore, I provide practical suggestions for policy advocacy purposes.

Chapter 8 regards special cases of bare indictments' deterrent effect against status-seeking actors, as I analyze a case that demonstrates how bare indictments frustrated dominance-seeking cyberattacks from Iranian actors without provoking a retaliatory response as would be predicted by SDT. I show that the theory holds even in this heightened setting wherein status-seeking arguably amounts to acts of cyber warfare. I then argue that the leverage of 'bare' criminal charges as a deterrent measure against acts of cyber warfare suggests a course of action in deterring the arguable acts of hybrid

warfare – combined kinetic and cyber war – waged by Russia against Ukraine in a conflict that is ongoing as of the time of this writing. Although the issuance of bare indictments to achieve extended deterrence would ordinarily be subject to the limitations of territorial jurisdiction, cross-national cooperation in technical attribution of cyberattacks is possible for deterring hybrid warfare. I give detailed policy suggestions as to how further leverage of the criminal indictment mechanism may achieve an efficient norm-setting deterrent effect even for cyberwarfare, given that classical CDT suggests that states' use of bare indictments as a deterrent measure for cyberattacks can serve to reaffirm state sovereignty.

Chapter 9 concludes the project by focusing on the theme of transcending boundaries. Just as cyberattacks blur national, jurisdictional, and conceptual borders, so too must the study of cyber deterrence transcend the boundaries between scholarly disciplines. Overall, the deterrent effect of bare indictments illustrates the role of domestic criminal law as a unilateral means of engendering international norm formation and asserting state sovereignty among the global order.

CHAPTER 2

FOUNDATIONAL CONCEPTS:

DETERRENCE, CYBERATTACKS, CRIMINAL LAW, AND STATUS

2.1.1. What is deterrence?

To understand why bare indictments deter cyberattacks, it is necessary to first have in mind a working definition of ***deterrence***. The definition this project uses draws from Alexander George's and Richard Smoke's seminal definition, but also supplements George's and Smoke's conceptualization by supplementing it with a defining aim. In George's and Smoke's 1974 book *Deterrence in American Foreign Policy: Theory and Practice*, deterrence is defined in the very first sentence of the first chapter: "In its most general form, deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits" (George and Smoke 1974, 11). Similarly, deterrence may here be defined as *the strategic shaping of an adversary's perception of the net costs and benefits expected to result from that adversary's committing an action in the future*, with the definitional aim of deterrence being *to convince that adversary not to commit that action in the future*.

From these definitions, deterrence might initially appear to be an overly broad concept, so diffuse that almost anything could be "deterrence." What distinguishes deterrence from other strategic routes? This is where turning to the definitional aim of deterrence helps to clarify what is *not* deterrence. Deterrence can be contrasted with – for instance – ***disruption***, which is stopping an adversary's action by making it infeasible (Borghard and Lonergan 2021, 23). If the adversary has already committed an attack, that

is called a ***deterrence failure*** (Mearsheimer 1985, 15). If deterrence has been successful, then the adversary must have been convinced not to commit the action. Where a disruption strategy would put a stop to the adversary's actions by making them infeasible, one example of a similar deterrence strategy might be to *convince* the adversary that the actions will be infeasible.

This illustrates an essential theoretical prediction of deterrence: *if an adversary expects the weighted costs of taking an action to outweigh the weighted benefits of completing that action, then the adversary will choose not to attempt that action in the future*. This broad principle and its corollary principles have spawned much scholarly attention. For instance, one of these corollary principles is that the adversary would not choose against taking that action – will not be ***deterred*** – unless the adversary *expects* that the costs will outweigh the benefits. Even if the costs will eventually outweigh the benefits in actuality, this fact alone is insufficient to achieve deterrence if the fact is not known to the adversary.

The following hypothetical illustrates why deterrent measures cannot deter unless the adversary knows in advance that the deterrent measure is in place. First, assume the following premise: the presence of a burglar alarm sometimes deters potential thieves. In the hypothetical scenario, a shopkeeper installs a burglar alarm at her shop. However, the shopkeeper does not make it known that the burglar alarm has been installed; she does not tell anyone else that she has installed the alarm, and she does not post any signs around the shop stating that there is a burglar alarm. That night, a thief breaks into the shop, so the alarm sounds. When the thief hears the alarm, the thief runs away without successfully stealing any property. The outcome of this scenario is that the thief was disrupted, as the

thief was prevented from *successfully* committing the theft; but the thief was not deterred, as the thief was not persuaded to refrain from committing the theft. Even though the premise "burglar alarms sometimes deter thieves" may still be true, this scenario shows that burglar alarms cannot deter thieves unless the presence of the burglar alarm is known in advance to the thief. This hypothetical illustrates the principle that deterrent measures cannot deter adversaries unless their presence is known in advance to the adversary. Knowledge is a necessary, though not a sufficient, condition for deterrence; although the potential thief knowing about the alarm in advance is not a guarantee that the potential thief will be deterred, the alarm cannot serve as a deterrent to the potential thief if the presence of the alarm is not known to the potential thief.

An integral part of achieving deterrence is instilling the adversary's *perception* that the costs will outweigh the benefits. Note that the adversary's perception, not the fact itself, is determinative to the deterrent outcome; the fact itself has no bearing on deterrence unless it is known to the adversary. Moreover, it is possible for the adversary to expect that the costs outweigh the benefits even though the costs would not outweigh the benefits in actuality. While this is possible, a related issue in deterrence studies is that of ***credibility*** (Quackenbush 2011, 746). If the costs would *not* outweigh the benefits in actuality, then how can the adversary be convinced that the costs *will* outweigh the benefits? On the other hand, where the costs *will* outweigh the benefits in actuality, how can this fact be communicated to the adversary so that the adversary will be convinced of this fact and hence be deterred? The credibility problem is central to one of the branches of deterrence studies that I identify in Subsection 2.1.3., and the policy solution posed by another branch of deterrence studies is discussed in Subsection 2.1.4.

2.1.2. Four directions for achieving deterrence

The mechanics of deterrence can be summarized and quantified by four conceptual variables. Returning to the core principle *if an adversary expects the weighted costs of taking an action to outweigh the weighted benefits of completing that action, then the adversary will choose not to attempt that action in the future* shows that deterrence is achieved via shaping the adversary's perceived cost-benefit calculus so that the expected weighted cost of committing the action exceeds the expected weighted benefit of committing the action. The terminology used in George's and Smoke's definition – "the **costs** and/or **risks** of a given course of action he might take outweigh its **benefits** [emphasis added]" – suggests four general directions that may, when leveraged individually or jointly, tip the perceived cost-benefit calculus such that, on net, the costs outweigh the benefits.

One, a deterrence strategy may seek to **lower the adversary's expected benefit** of committing the action. Turning back to the hypothetical of the thief, assume that the thief is motivated by monetary profit. In the thief hypothetical, an example of lowering the adversary's expected benefit would be persuading the thief that there is almost no cash in the register and that the items in the shop are of very little monetary value.

Two, a deterrence strategy may **raise the adversary's expected cost** of committing the action. These costs could be before-the-fact or after-the-fact. Shaping the adversary's perception regarding before-the-fact expected costs could include making the thief realize that in order to commit the theft, the thief must invest in expensive equipment needed to stage the break-in of the shop. After-the-fact expected costs could include jail time. In

deterrence studies parlance, this second direction is termed ***deterrence by punishment*** (Mazarr 2021, 15-16).

Three, a deterrence strategy may **lower the adversary's expected probability of benefit** from committing the action. For instance, if the thief expects that it will be very difficult to commit the theft –perhaps the thief expects that it will be very difficult to break into the store, open the cash register, or move the merchandise out – the thief may choose not to commit the theft. In deterrence studies parlance, this third direction is termed ***deterrence by denial*** (Mazarr 2021, 15).

Four, a deterrence strategy may **raise the adversary's expected probability of cost** from committing the action. An example of expected probability of cost would be not the expected cost of jail time itself, but rather, the likelihood that the thief will be jailed.

Essentially, the aim of deterrence can be mathematically modeled via a simple inequality that integrates the four variables covered above. The aim of deterrence is to make the following inequality true:

$$(P_C)(C) > (P_B)(B)$$

with (P_C) being the adversary's expected probability of cost, (C) being the adversary's expected cost, (P_B) being the adversary's expected probability of benefit, and (B) being the adversary's expected benefit. (P_C) is multiplied by (C) to arrive at the adversary's expected weighted cost from committing the action, and (P_B) is multiplied by (B) to arrive at the adversary's expected weighted benefit from committing the action. This inequality, with the adversary's expected weighted cost being more than the adversary's expected weighted benefit, represents the condition that must be true for deterrence to be achieved.

Using the expected probabilities to weight the expected cost and expected benefit is important because even if the expected cost were astronomically high, expected cost would not serve as a deterrent if the adversary also expected a very low likelihood that the expected cost would ever be imposed. For example, if an adversary expects that the penalty for the action of shoplifting will be five billion U.S. dollars ($5,000,000,000.00) but the adversary also expects that there is an infinitesimal likelihood that this penalty will ever be imposed upon the adversary – say, one out of 333 million, with 333 million being more than the estimated population of the U.S. according to the 2020 U.S. census (U.S. Census Bureau 2021) – then even this very high expected cost will be unlikely to deter the adversary from choosing to commit the action of shoplifting.

2.1.3. Branches of deterrence theory

From the theoretical framework of deterrence, a wide-ranging scholarly literature has developed. Deterrence studies can be broadly categorized into three major branches: nuclear, military, and criminal. Although there is much conceptual overlap, certain specialized features can be identified to distinguish each branch.

The word "deterrence" may call to mind (Mazarr 2021, 18, at footnote 14) the first branch, ***nuclear deterrence theory*** ("NDT"). Nuclear deterrence theory is the branch of deterrence studies that deals with deterring attacks committed using nuclear weapons. NDT's inception can be traced to the mid-twentieth century, with the development and advent of nuclear weapons (Knopf 2010, 1). One of the specialized core features that distinguishes NDT from other branches of deterrence studies is the doctrinal concept of ***mutual assured destruction*** ("MAD"). Mutual assured destruction in NDT refers to the

strategy of achieving deterrence by establishing the capability and the willingness to completely destroy the adversary if the adversary mounts a nuclear attack (Quackenbush 2011, 746). MAD is traditionally modeled via the game of "Chicken" (Zagare 1990, 243), a symmetric game in which both players are deterred. Therefore, MAD as a deterrence strategy operates via the second direction presented above, raising the adversary's cost; each of the two players seeks to persuade the adversary that the adversary will suffer devastating costs if the adversary chooses to mount a nuclear attack. However, a major issue that is at least theoretical if not also empirical regards the fourth direction discussed in the preceding subsection: maintaining the adversary's expected probability of cost. Even if a player has the capability to impose devastating costs on its adversary if that adversary mounts a nuclear attack, how likely is it that a player will have the willingness to impose those costs on the adversary if the adversary does indeed choose to mount a nuclear attack? Recall that deterrence strategies hinge on the adversary's perception of information, not the information itself; thus, the more important issue becomes how the adversary may be persuaded of the player's willingness. As mentioned before, this issue is referred to as the ***credibility*** problem in NDT (Mearsheimer 1985, 18).

Scholars have observed that NDT tends to overshadow the second branch of deterrence, as the very term "deterrence" is frequently taken to mean *nuclear* deterrence (Mazarr 2021, 18, at footnote 14) and deterrence studies in the late twentieth century frequently focused on deterrence in the context of preventing nuclear war (Knopf 2010, 1). In deterrence studies, a second branch of deterrence is known as "conventional deterrence"; for clarity of terminology, I will refer to conventional deterrence as ***military deterrence theory*** ("MDT"). Military deterrence theory is the branch of deterrence studies

that deals with deterring attacks committed using conventional military forces (which is to say, not guerrilla forces) and non-nuclear weapons. One of the seminal works on MDT, if not *the* seminal work, is John J. Mearsheimer's 1983 book *Conventional Deterrence*. The definition Mearsheimer uses for the purposes of his study indicates that MDT and NDT share a common foundation: "Deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the costs and risks" (Mearsheimer 1985, 14). However, when defining the scope of his work, Mearsheimer distinguishes MDT from NDT by noting that the concept of MAD and the issue of credibility, while not necessarily absent, are not as pertinent to a conventional military context (Mearsheimer 1985, 18).

Besides the definitional feature of dealing with conventional military forces and non-nuclear weapons, and the negative distinguishing feature of MDT's focus being shifted away from MAD and credibility, a positive distinguishing feature of MDT has been identified by James J. Wirtz in his 2018 article "How Does Nuclear Deterrence Differ from Conventional Deterrence?" Wirtz identifies "contestability" as a distinguishing feature of MDT. NDT deals with a context of nuclear war, in which a "nuclear attack involving more than a few nuclear weapons" (Wirtz 2018, 62) is *incontestable*. A player might be able to retaliate, but not defend; there is no defense to a full-scale nuclear attack (Wirtz 2018, 62), whether as a first strike by an adversary or as a retaliatory strike by the main player. By contrast, a military offensive may be *contestable*; each player might be able to directly defend against the other's military offensive, without having to counterattack by wreaking destruction upon the adversary.

The means of achieving deterrence can comprise more than just nuclear weapons or military forces, as other deterrent measures may be available to a state. Michael J. Mazarr's 2021 article "Understanding Deterrence" identifies a few examples: "A **state** can deter using threats of economic sanctions, diplomatic exclusion, or information operations [emphasis added]" (Mazarr 2021, 18). Together, the branches of NDT and MDT are part of a larger branch of deterrence studies that I term ***state deterrence theory*** ("SDT"). This terminology is in accordance with the larger branch's focus on the deterrent measures available to a nation-state actor or nation-state-like actor to deter another state actor. Thus, state deterrence theory is the larger branch of deterrence studies that deals with the deterrence of state actors – a category that includes, as will be further explored later, individual actors or small groups who act *on behalf of* a state – and state-like actors.

The third branch of deterrence theory is ***criminal deterrence theory*** ("CDT"). Criminal deterrence theory is the branch of deterrence studies that deals with deterring harm-causing actions that a state or a state-like governmental body has deemed to be crimes (Bentham [1789] 1823, 171). Generally speaking, the major feature that distinguishes CDT from SDT regards the identity of the adversary or – to use the terminology of George and Smoke – "opponent." CDT assumes that almost any actor – not just a state actor or state-like actor – is capable of committing a crime. By contrast, any actor capable of mounting a full-scale nuclear attack or a military incursion would arguably be characterizable as a state actor or state-like actor. While state actors can commit crimes, not all targets of criminal deterrence are necessarily states.

Despite the distinguishing features of the branches I have identified, SDT and CDT share much in common, as they operate from a shared mechanistic framework. In effect,

then, it is surprising that little scholarly literature engages with both SDT and CDT to harmonize the two branches and consider how insights from one of the branches could be beneficial to the other. For example, in Lawrence Freedman's book *Deterrence* (2004), the author notes, "What is striking is how similar the debates are in the strategic studies and criminological communities, yet how little they draw upon each other's work" (60).

CDT has its roots in the eighteenth century, with the writings of the two "classical criminologists" (West 2017, 1) Cesare Beccaria and Jeremy Bentham. The founding work of CDT is Beccaria's 1764 treatise *Dei delitti e delle pene*, which translates to *On Crimes and Punishments*. Bentham was greatly influenced (Hart 1982, 43-44) by the CDT principles that Beccaria proposed in *On Crimes and Punishments*; Bentham advanced and further developed CDT's principles in *Introduction to the Principles of Morals and Legislation* ([1789] 1823), *Rationale of Punishment* (1830), and *Theory of Legislation* (1871). CDT, with its focus on how to achieve efficacy of punishment, arose against a context of failing criminal justice systems across eighteenth-century Europe (Rosen 1999, 180). The classical criminologists argued that a state's allowing most criminal offenders to go free yet imposing excessively cruel punishment on a handful of criminal offenders was not only ineffective, but also counterproductive (Beccaria 1764b, 13-14).

In the late 1960s, interest in CDT revived with empirical studies in economics and criminology. Economist Gary S. Becker's 1968 article "Crime and Punishment: An Economic Approach" has been cited as the seminal article of neoclassical CDT (Chalfin and McCrary 2017, 23). Becker articulated CDT principles in formal economic terms such as expected utility and optimality (1968). Through the second half of the twentieth century and the start of the twenty-first, studies in the CDT branch of deterrence have often tested

to what extent the essential principles of CDT hold true. Today, the wide-ranging body of scholarly work on CDT includes economic and game-theoretic models, behavioral psychology studies that focus on the perception of the potential offender, and criminological tests using empirical data. Modern CDT studies continue to engage with eighteenth-century CDT principles. Thus, the following subsection gives an overview of the relevant theoretical propositions of classical CDT.

2.1.4. Relevant theoretical principles of classical CDT

If criminal deterrence strategies were never to fail, then punishments would never have to be imposed. These would be ideal circumstances: a society in which no harm-causing crimes ever occurred. However, considering CDT's core assumption that anybody – whether a person or entity, whether a member of the society or someone foreign to it – is capable of committing a crime, the sheer number of adversaries that are to be deterred reveals that the complete absence of harm-causing crimes is so improbable as to be impossible.

When the field of possible adversaries is expanded from the roughly numerable 'states or state-like actors' to the multitudinous 'almost anyone,' the goal of CDT cannot be to achieve complete deterrence, but rather, to achieve ***optimal deterrence***. Optimal deterrence means, given the amount of resources expended on deterrence, maximizing the deterrent effect (Bentham 1830, 27; Sunstein et al. 2000, 237). A component of maximizing the deterrent effect means minimizing how many deterrence failures occur (Becker 1968, 5).

There are two types of criminal deterrence: ***specific deterrence*** and ***general deterrence***. Specific deterrence means deterring the actor who committed that offense, such that this actor is convinced not to commit that offense in the future (Bentham 1830, 19).[1] General deterrence means deterring the members of the pool of actors who are capable of committing that offense, such that these ***potential offenders*** are convinced to not commit that offense in the future (Bentham 1830, 19).

Although optimizing deterrence means that some deterrence failures are to be expected, classical CDT posits that the key to achieving optimal deterrence lies in the state's response to those deterrence failures (Beccaria 1764a, 31; Beccaria 1764b, 24). To achieve optimal deterrence, there are two necessary elements to the state's response when a deterrence failure occurs. One, the state must determine the perpetrator of that crime and impose punishment upon the perpetrator (Bentham 1830, 29). Two, the state must ensure that this punishment is not kept secret; when the imposition of punishment is made known to the public, the general deterrent effect will be enhanced (Beccaria 1764b, 24; Bentham 1830, 30).

Classical CDT predicts that the first element – state imposition of punishment upon an actor who has committed a criminal offense – is likely to achieve specific deterrence of that offense's perpetration by the actor (Beccaria 1764a, 31). Meanwhile, the second element – making the state imposition of punishment publicly known – is likely to achieve general deterrence of that offense's perpetration by members of the pool of potential offenders, as membership in this pool is synonymous with being a member of the public.

[1] "The prevention of offences divides itself into two branches: *Particular prevention*, which applies to the delinquent himself; and *general prevention*, which is applicable to all the members of the community without exception [italics Bentham's]" (Bentham 1830, 19).

Recall that for any deterrent measure to serve as a deterrent measure, the presence of the deterrent measure must be known in advance to the adversary. Likewise, for an imposition of punishment to serve as a measure of general deterrence, the imposition of punishment must be known to the public, and cannot be kept secret (Bentham 1830, 30).

This can be connected to the credibility problem in NDT. Recall that disruption is another strategy that can be contrasted with deterrence, and that an example of a deterrence strategy similar to disruption is *convincing* the adversary that the actions will be infeasible. Infeasibility can be likened to raising the adversary's expected cost, but the problem of credibility may depress the adversary's expected probability that those costs will be imposed if the adversary decides to commit that offense. In its response to deterrence failures, classical CDT poses a way to counteract the credibility problem.

According to classical CDT, a credible way to convince an adversary that the costs will be imposed is to follow through on imposing those costs upon other adversaries who have committed that offense (Bentham 1830, 29). Beccaria and Bentham predict that the publicly known imposition of punishment upon some adversaries, for whom specific deterrence has already failed because they have indeed committed that offense, is likely to achieve general deterrence by raising the expected weighted cost of all adversaries capable of committing that offense. Bentham and Beccaria theorize that when it becomes known to members of the pool of potential offenders that an actual offender was punished, then they can be persuaded that they too will likely be punished if they choose to commit the offense (Beccaria 1764a, 31; Beccaria 1764b, 24; Bentham 1830, 20).[2] In the cost-benefit calculus

[2] "General prevention is effected by the denunciation of punishment, and by its application, which, according to the common expression, *serves for an example* [italics Bentham's]. The punishment suffered by the offender

of any potential offender, the knowledge of the punishment itself can be factored in as an increase in the expected cost, while the knowledge that the punishment was actually imposed addresses the credibility problem because it can be factored in as an increase in the expected probability of cost. Thus, imposing punishment and making the imposition of punishment publicly known can serve as a general deterrent measure because it raises potential offenders' expected weighted cost.

According to Bentham, the state's response can also achieve specific deterrence upon the criminal offender henceforth, because the offender will likely be convinced that the offender will again be punished if the offender again commits such a criminal offense (Bentham 1830, 20). Beccaria and Bentham predict that actual imposition of punishment (Beccaria 1764a, 31; Bentham 1830, 20) upon an individual who has committed a given offense will deter that adversary from committing ***recidivist offenses***, which are repeat offenses by the actor responsible for committing the crime.

To summarize, the ideal circumstances are where the state never has to impose punishment because no harm-causing crimes ever occur. These ideal circumstances are impossible when the pool of potential offenders has an innumerably large membership. Beccaria and Bentham theorize that publicly known imposition of punishment upon actual offenders is likely to deter potential offenders because potential offenders are likely to be convinced that they too will be punished by the state if they commit similar offenses. Therefore, when a deterrence failure inevitably occurs, the state should impose punishment upon the criminal offenders to promote specific deterrence of recidivist offenses, and the state should make its imposition of punishment publicly known to

---

presents to every one an example of what he himself will have to suffer if he is guilty of the same offence" (1830, 20).

promote the establishment or maintenance of general deterrence. Following through on the imposition of costs and then making this imposition known can achieve both specific deterrence of the individual who committed the offense and general deterrence of the other potential offenders.

2.1.5. Modern CDT on "informal sanctions" as a deterrent measure; probability of apprehension as trigger of informal sanctions

The preceding subsection referred to the role of "state imposition of punishment" as one of the necessary elements that classical CDT suggests is necessary to achieve and optimize deterrence. Starting in the late twentieth century, some economic and criminological approaches to CDT have yielded an elaboration regarding what can serve as "state imposition of punishment." Modern CDT scholars have theorized that it is not only the formal legal consequences, such as jail time or a monetary fine, that can be the "punishment" which is the deterrent measure in CDT. ***Informal sanctions***, which are the extralegal negative consequences that the potential offender can expect as a result of being subject to the governmental criminal justice process, can also serve as punishments. When these informal sanctions are visibly imposed by the state against individuals who have committed an offense, the informal sanctions can be quantified as part of the adversary's expected weighted cost. Examples of informal sanctions include negative internal feelings of shame, guilt, or embarrassment (Jacobs et al. 2000, 173); social ostracization (Williams and Hawkins 1986, 564); disapproval from valued associates, such as family and friends (Anderson et al. 1977, 107); and damage to reputation (Williams and Hawkins 1986, 562-564). According to a 2000 criminological study by Bruce A. Jacobs, Volkan Topalli, and

Richard Wright, some CDT scholars even take the position that the governmental criminal justice process only achieves deterrence "insofar as it triggers informal sanctions," as opposed to formal legal consequences (quoted in Jacobs et al. 2000, 171). Jacobs, Topalli, and Wright continue by emphasizing the significance of the concept of informal sanctions in modern CDT: "The notion that informal sanction threats influence criminal decision-making is perhaps the most important contribution to deterrence theory in the past 15 years" (2000, 171).

Relatedly, many CDT scholars have recognized that informal sanctions can be triggered by an earlier stage in the governmental criminal justice process, namely apprehension. The focus on the apprehension stage represents another conceptual refinement from classical and neoclassical CDT. For example, Becker's economic neoclassical model of CDT (1968) considered formal legal consequences; therefore, it made sense for Becker to quantify the adversary's expected probability of cost *(P_C)* as the ***probability of conviction***. Conviction means a legal determination, usually by a court of law, that an adversary was indeed the perpetrator of a crime and therefore has violated the criminal law (Legal Information Institute, "Conviction," n.d.). It is only upon conviction that formal legal consequences, such as imprisonment or monetary fines, can be legally imposed. Because the cost of formal legal consequences can only be imposed if the offender was convicted, and Becker's model used formal legal consequences as the expected cost, Becker's model (1968) assumed that the probability of conviction would be the correct value for the potential offender's expected probability of cost *(P_C)*.

By contrast, a 1986 criminological study by Kirk R. Williams and Richard Hawkins pointed out that informal sanctions may frequently be imposed upon arrest (1986, 558 at

footnote 12; 1986, 562-564). Williams and Hawkins theorized that others in society would tend to stigmatize a person who had been arrested on suspicion of committing a crime; as this stigma could lead to loss of social status as well as actual loss of relationships with personal acquaintances or business associates (1986, 562). Assuming that such informal sanctions could, in actuality, be triggered by arrest, the informal sanctions could serve as the underlying reason that potential offenders might be generally deterred by the expectation of arrest. The arrest is the *imposition* of punishment, but the arrest is not itself the punishment; just as conviction is not in itself a punishment, but conviction triggers the punishment of formal legal consequences, apprehension triggers the punishment of informal sanctions. Therefore, when informal sanctions are quantified as the adversary's expected cost, the appropriate corresponding value for the variable *(P_C)* is not the probability of conviction, but rather, the ***probability of apprehension***. Apprehension means that the adversary is detained by state agents because there is some reason for the state to suspect that the adversary has committed a particular criminal offense (Nagin 2013, 206). An arrest is a formal type of apprehension, but – as will be discussed later in this subsection, in the case study of a Japanese national who was detained on suspicion of having violated the criminal law – not all apprehensions are necessarily arrests.

Summarizing their theoretical propositions for further empirical testing by subsequent scholars, Williams and Hawkins wrote that informal sanctions could serve as a general deterrent measure when the potential offender quantified some combination of informal sanctions as an expected cost *(C)* and also expected a high probability of apprehension *(P_C)*:

> We would predict that general deterrence is more likely to operate when a person perceives a high probability of arrest and (1) when others disapprove of or

> generally discredit the potential offender, thus creating a reputational stigma of arrest, (2) when the arrest is perceived as possibly jeopardizing relationships with significant others, or (3) when the arrest is seen as possibly destroying past accomplishments and/or future opportunities (1986, 565-566).

From this quote, it can be observed that the modern CDT literature on informal sanctions resonates with the classical CDT framework on state imposition of punishment. The difference is that where classical CDT focused on formal legal consequences as an expected cost, modern CDT recognizes that extralegal consequences of being subject to the state's governmental criminal justice process can also be quantified as an adversary's expected costs. One could also observe that making the imposition of punishment publicly known plays an even more crucial role than it did in classical CDT. Informal sanctions are frequently comprised of the disapproval of others in a society. Thus, making the imposition of punishment publicly known is not only optimal for the general deterrent effect, but is also instrumental in the functioning of informal sanctions. It is only when others in society know about the imposition of punishment, with arrest being the imposition of punishment, that those other members of society could exercise social disapproval in response.

One of the scholars to empirically validate Williams' and Hawkins' propositions was statistical criminologist Daniel S. Nagin. In a 2013 economic meta-analysis, Nagin found that the empirical evidence on criminal deterrence "pertains almost exclusively to apprehension probability"; overwhelmingly, empirical tests indicated that it was the probability of apprehension – not the probability of conviction – that was determinative in whether any deterrent effect was achieved. Nagin elaborated that apprehension triggers costs that are not part of the formal legal consequences yet can properly be quantified as an expected cost of the potential offender; expected costs that would be imposed upon apprehension "include the unpleasantness of the apprehension itself, possible loss of

liberty due to pretrial detention, and legal fees. Perceived cost of apprehension also includes the social and economic costs triggered by arrest, even without conviction, such as disapproval of family, friends, and the community at large, as well as job loss" (2013, 210).

A case study described by legal scholar Mark D. West further demonstrates why the informal sanction of practical consequences imposed upon apprehension can serve as a specific deterrent measure even in the absence of a conviction. West relates this case study in the context of a 2003 study on Japan's lost-and-found property law. The Japanese police had reason to suspect that an individual had violated the criminal law on misappropriation of property, so the police requested that the individual come in for questioning. The facts indicate that the individual had indeed violated this criminal law, as he "immediately admitted" his actions upon speaking to the police (West 2003, 390). This individual was apprehended, because he was detained on suspicion of having violated a criminal law, but he was not formally arrested (West 2003, 390). Ultimately, there was no conviction – no formal determination that he had violated the law, and hence no imposition of formal legal consequences – but as a result of being subject to the governmental criminal justice process, the individual "spent a total of 12 hours with police on three separate occasions and missed two days of work" (West 2003, 390). Speaking to West, the individual proclaimed that the costs of apprehension had specifically deterred him from henceforth committing actions that could constitute a violation of that criminal law: "The whole process… didn't change my morals… But it was such an ordeal that I'll never do anything like that again" (West 2003, 391).

To summarize, modern CDT posits that apprehension triggers informal sanctions, which "for some offenders may be even more costly than the formal sanctions" (Nagin

2013, 210). Given the importance of informal sanctions as an expected cost *(C)*, it is often appropriate to correspondingly quantify expected probability of cost *(P_C)* as the probability of apprehension rather than the probability of conviction. Empirically, it has been validated that potential offenders tend to consider the probability of apprehension, not the probability of conviction, as determinative of the deterrent effect; there is also empirical evidence that informal sanctions tend to predominate in an adversary's calculation of expected costs.

There is some experimental evidence that the predominance of informal sanctions in an adversary's cost-benefit calculus holds true for cyber adversaries. Criminologist Adam M. Bossler tests the deterrent effect of informal sanctions in a statistical study that administers a survey to a sample of undergraduate students. From his experiment, Bossler finds that the expectation of informal sanctions is correlated with decreased willingness to commit various types of cyberattacks, whereas the expectation of formal sanctions was not predictive of willingness to commit cyberattacks (2019, 611). Discussing the limitations of his study, Bossler notes the emergence of ideologically motivated cyberattackers (Bossler 2019, 599-601), who might be more difficult to deter than the sampled undergraduates. In this context, Bossler also remarks that relatively "little empirical research" has tested the propositions of CDT as applied to cyber matters (2019, 599). Indeed, scholarly discussions of deterrence in the cyber domain largely approach the subject from a SDT rather than CDT perspective.

///

///

2.2.1. What is cyber deterrence? What is a cyberattack?

With "deterrence" defined, ***cyber deterrence*** might be defined as *the deterrence of cyberattacks*, but this prompts the need to define a "cyberattack." To account for the valuable nature of data in the cyber domain, this project defines ***cyberattacks*** as *actions obtaining unauthorized access to computer systems and / or using cyber means to cause damage to computer systems.* This subsection discusses and justifies the definition of cyberattacks.

Scholars have noted that the definitional issue can engender confusion when the foundational need to establish what concept to which the use of cyber deterrence terminology purports to refer is arguably overlooked. For instance, military strategist Timothy M. McKenzie argues that "Senior civilian and military leaders often use the term *cyber attack* incorrectly" (2017, 3), pointing to an example of using an "extremely broad definition" as contrasted with McKenzie's narrower conceptualization (2017, 4).

A starting point for the definition of "cyber attack" might be Aaron F. Brantly's categorization. Brantly sorts "cyberspace operations" into "three broad categories": "cyber attacks, cyber espionage, and cyber theft," with "cyber attacks" defined as "those acts in cyberspace that degrade, deny, or destroy" (2018, 40). Brantly argues, "Deterrence by threat within cyberspace is realistically only applicable to cyber operations that result in direct physical effects…" (44) but also notes, "Cyber deterrence has fundamental problems including the realization that the most valuable assets in cyberspace might not be destroyed or degraded, but rather stolen and used" (43). If cyber deterrence is to prevent a broader scope of undesired actions than just those activities that "degrade" or "destroy,"

then either cyber deterrence must aim to deter more categories of cyber operations than just "cyber attacks," or "cyber attacks" should be more broadly defined.

McKenzie's treatment of the definition of "cyber attacks" goes with the latter option; McKenzie conceives of cyber deterrence as targeted toward preventing only "cyber attacks" rather than also other categories of cyber operations (2017, 5), but McKenzie broadens the definition of "cyber attacks" to read "the deliberate damage, destruction, or corruption of critical private systems or critical/noncritical government systems or any cyber activity that results in a significant financial loss to a US private company or US government office/agency or that results in death, destruction, or serious injury" (2017, 4-5). McKenzie compares his definition to that of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*: "a cyber operation, whether offensive of defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (2017, 4). According to McKenzie, Panayotis A. Yannakogeorgos "refers to actions that fall below the threshold of cyber attack as aggressive incidents" (2017, 4) and "The United States Cyber Command (USCYBERCOM) groups cyber activity into the three categories of access, disruption, and attack" (2017, 4); building from these conceptualizations, McKenzie argues that "some activities categorized as a 'disruption' or 'aggressive incident' could also rise to the level of a cyber attack, depending on the economic impact" (2017, 4). Hence, McKenzie's broader conceptualization of "cyber attack" captures those cyber operations that have significant financial consequences.

Might there be an even more broadly inclusive criterion by which to systematically define the "cyber attack"? For two reasons, McKenzie's results-oriented definition of "cyber attack" arguably remains too under-inclusive. First, defining cyberattacks in terms

of "significant financial loss to a US private company or US government office/agency" overlooks a major category: the non-financial harm, such as psychological detriment to individuals by perception of the breach of privacy or infringement upon the sovereignty of public actors, that may be caused by undesired cyber operations. Second, McKenzie's definition is too focused on *measurable* financial harm, and could be improved by accounting for the highly valuable yet also difficult-to-value nature of data.

In privacy law and information studies, data is often conceptualized as a valuable commodity whose mere disclosure carries the potential for misuse. Privacy law scholar Daniel J. Solove's 2011 book *Nothing to Hide: The False Tradeoff between Privacy and Security* reveals the need of privacy by showing that even "seemingly innocuous data," once made known, can be used for unwanted purposes (27). Solove presents a hypothetical involving it being made known that someone has purchased a book about cancer and has also purchased a wig; "combine these two pieces of information," says Solove, and now the inference can be made that you have cancer and are undergoing chemotherapy" (27). To extend Solove's hypothetical, a second-order inference can be made that has the potential to be even more damaging. If this person is undergoing chemotherapy, it could further be inferred that this person probably goes to regularly scheduled chemotherapy appointments. To a malicious actor, the inference about the regular appointments could present a recurring opportunity to exert psychological pressure on the person, or to steal something from the person while the person's attention is otherwise occupied.

Although McKenzie's definition includes "economic harm," the case of exerting psychological pressure shows that certain cyber operations – even just what under McKenzie's definition would be labeled "access," which is not included as a target of cyber

deterrence – can result in harm that is not directly financial in nature. A second, related issue persists even if it assumed that data has some value. Many have described data as the "'oil' of the digital economy" (Spiekermann and Korunovska 2016, 1; see also Aslam and Shah 2020, 11), and large multinational technology companies treat data as a tradable asset (Spiekermann and Korunovska 2016, 2; Aslam and Shah 2020, 11). However, much more so than with tangible physical commodities like oil, a number of conceptual issues make data notoriously difficult to value in monetary terms (Aslam and Shah 2020, 12-13; Spiekermann and Korunovska 2016, 2). At the extreme end, according to Aqib Aslam and Alpa Shah, "some countries and companies claim that user data has no value until it has been processed – before then data is worthless" (2020, 7). If the monetary value of user data has to be numerically quantified, and aggregated to a "significant financial loss," before it can be included within what McKenzie's definition would consider to be a "cyber attack" and therefore a target of cyber deterrence, then the widespread argument that data is worthless or of *de minimis* monetary value excludes a large class of harmful cyber operations from being targets of cyber deterrence. A third issue here, which speaks to the technical computer science realities of cyber deterrence, is this: even if the actor that initially gained access to the data did not use the data to carry out any malicious action, the action of access opens a 'backdoor' or point of entry that can be exploited by other – potentially malicious – actors (Jensen 2012, 788).

Data, no matter how seemingly innocuous, carries value.[3] Moreover, it is not simply that the excluded types of harmful cyber operations described above are types that *should*

[3] For further reading on the monetary and intelligence value of seemingly innocuous bits of digital data, see Matt Burgess' analysis of a corporate practice called browser fingerprinting: "The Quiet Way Advertisers are Tracking Your Browsing" (Burgess, February 26, 2022).

be a proper target of cyber deterrence if possible. They also provide a consistent way to define the cyberattack.

Observe the following diagram, a spectrum of cyber operations in accordance with the U.S. Cyber Command's categorization (McKenzie 2017, 5):

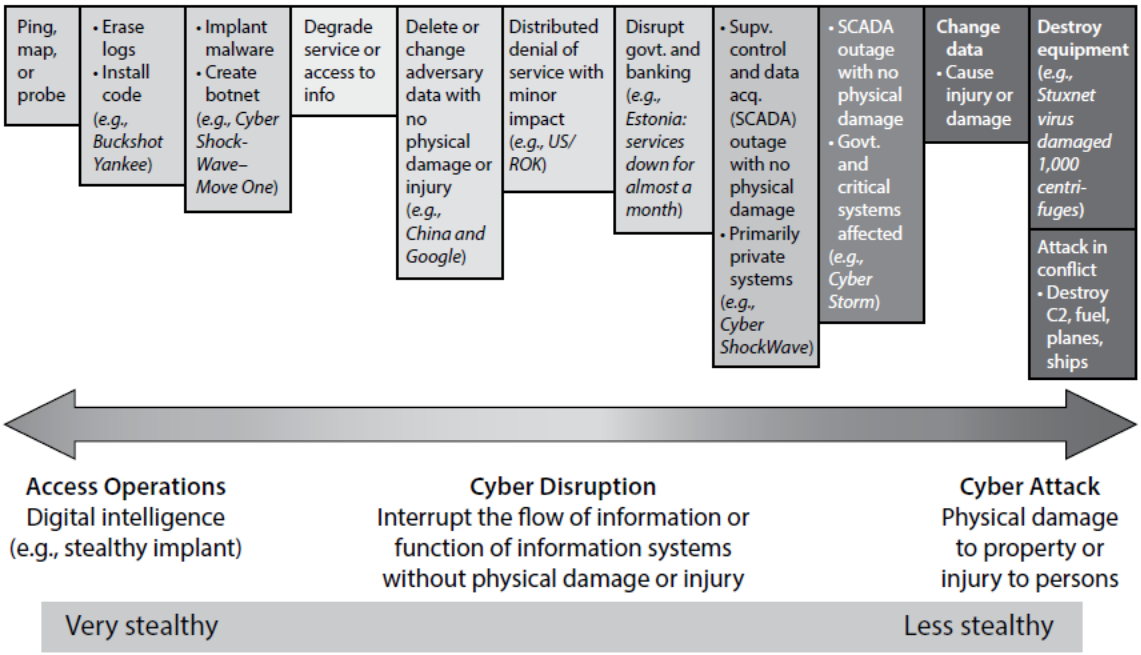


Figure. Spectrum of cyber operations. (Adapted from USCYBERCOM/Judge Advocate, briefing, subject: Assessing Actions along the Spectrum of Cyberspace Operations, slide 18, no date.)

One common theme that emerges across the "cyber operations" on McKenzie's spectrum is the involvement of unauthorized access to computer systems. Toward the left side of the spectrum, the cyber operation described is the access itself. The example given on the rightmost side of the spectrum is the Stuxnet attack. Stuxnet affected the computerized systems that controlled Iran's nuclear centrifuges, apparently causing the centrifuges to spin out of control and explode (Kushner 2013). Even cyberattacks of Stuxnet's extreme severity involve, as a necessary component, the unauthorized access of a

computer system. The access in question need not be remote access; the Stuxnet virus is thought to have been originally introduced to computerized systems not remotely, but rather, via the physical on-site insertion of a USB Type-A flash drive (Kushner 2013).

For the "cyberattacks" that are to be deterred, then, this project will use the following definition: *Cyberattacks are actions that obtain unauthorized access to computer systems and / or use cyber means to cause damage to computer systems.*

This definition aims to avoid both under-inclusivity and over-inclusivity. It is not under-inclusive, because unauthorized access to electronic systems is a component common to malicious cyber operations. Neither is it over-inclusive, since this definition also puts the focus on deterring actions inextricably tied to the cyber domain, rather than arguably better characterized as merely carried out through electronic means. For instance, this definition tends not to include actions that might be more aptly characterized as drone strikes, wire fraud, or illegal downloading.

The use of this definition bears at least two further advantages. First, the formulation of a deterrence theory that deters "cyber attacks" defined broadly rather than narrowly – using a broad definition of "cyber attack" to encompass operations of low-level severity rather than only those that are highly severe in terms of the amount of destruction caused – enables the potential that the theory will, in turn, be more broadly applicable. For a point of comparison, this is an enhancement because it would be comparable to developing a policy mechanism that would be effective against deterring "theft" – petty theft and grand theft alike – rather than only grand theft. Second, the definition's focus on "unauthorized access to electronic systems" suggests an intervention point for a theory of cyber deterrence to leverage.

At the same time, the definition still integrates emphasis on the damage that can be caused via cyber means yet might be argued to not involve unauthorized access. An example of a cyber operation that meets the second part and not necessarily the first part of this project's definition of cyberattacks is the ***distributed denial of service ("DDoS")*** cyberattack. A DDoS cyberattack floods computer systems with junk traffic, rendering those computer systems inaccessible (Fortinet 2022). To use the shopkeeper hypothetical, the DDoS cyberattack could be analogized to a mob of people following a malicious order to enter the shop, physically filling the shop with people. The people in the mob do not purchase anything while inside the shop. The mob's coordinated effort to fill the shop renders the shop entirely inaccessible to customers who would want to make purchases; this causes damage because it renders the shop inoperable.[4]

As Martin C. Libicki writes, "unauthorized access" is frequently the necessary first step in a malicious cyber operation (Libicki 2009, 15-16). A cyberattack may not only be an act of cyber warfare, but can also enable other malicious actions such as data theft, in which confidential digital information or a copy thereof is taken. Moreover, there are a variety of difficult-to-value harms associated with the unauthorized access itself. Not only does a cyberattack tend to be an instrumental step in causing harm, but a cyberattack can itself cause harm. To encompass the nature of the harm that can be caused by a cyberattack, the broad definition used in this project centers on two types of actions: obtaining unauthorized access to computer systems and using cyber means to damage computer systems.

[4] For further discussion of why U.S. federal cybersecurity law considers DDoS attacks' "impairment" of computer operations to be a form of "damage" to computer systems, see cybersecurity attorney Shawn E. Tuma's analysis (2013).

2.2.2. The problem of technical attribution in cyber deterrence; attribution by indictment

Just as NDT scholarship has the central issue of the credibility problem, cyber deterrence scholarship has its own central issues. One of these central issues – if not *the* central issue – is the problem of ***technical attribution***. Technical attribution means determining who was the actor that executed a cyberattack (Healey 2011, 57).

Approaching cyber deterrence by applying the principles of SDT, Libicki in his monograph book *Cyberdeterrence and Cyberwar* (2009) contrasted cyber deterrence with SDT to show why technical attribution was a unique concern for the cyber domain. In the nuclear domain, it is usually obvious that a nuclear attack emanated from a certain geographic location; this made determining the source of a nuclear attack straightforward in NDT (Libicki 2009, xvi). Moreover, only a state or state-like actor would be capable of mounting a large-scale nuclear attack, so the state whence the nuclear attack emanated would be the actor that executed the nuclear attack; attribution of nuclear attacks would not need to consider non-state actors operating in that geographic location (Libicki 2009, xvi). Likewise, when adapting principles from the military domain, technical attribution would be among cyber deterrence's "significant barriers" that normally would not be considered in the context of a MDT analysis (Libicki 2009, xix).

Similarly, cybersecurity analyst Emilio Iasiello presents technical attribution as a theoretical obstacle for cyber deterrence and argues that this theoretical obstacle will prove "insurmountable" for the practice of cyber deterrence (2014, 67). Expressly contrasting cyber deterrence with SDT models of "nuclear deterrence, terrorism deterrence, and rogue state deterrence" (2014, 60-63), Iasiello explains that knowing what

actor executed the action to be deterred is a necessary prerequisite to "launching a retaliatory strike" (65). Iasiello presented technical attribution as the result of technological limitations, stating "It is extremely difficult to determine [technical] attribution in cyberspace where savvy operators have a multitude of obfuscation techniques to thwart defenders from correctly identifying their true point of origin" (2014, 58).

Unlike Iasiello, who presented technical attribution as an insurmountable hurdle for cyber deterrence, legal scholar Eric Talbot Jensen in a 2012 law review article entitled "Cyber deterrence" presented the technical attribution problem in a more delimited fashion. Although Jensen acknowledged that technical attribution was "one of the most vexing problems" for cyber deterrence, he pointed out that most cyberattacks would be technically attributable "with sufficient time and resources" (2012, 786). Jensen argued it was not that technological limitations would render technical attribution impossible, but rather, that technical attribution was non-obvious in cyber operations. Thus, the problem is best characterizable not as technical attribution, but as *prompt* technical attribution (Jensen 2012, 786). Although Jensen's study approached cyber deterrence from a legal perspective, the body of law upon which Jensen's study centers is the international laws of war (796) rather than domestic criminal law. While a cyber deterrence study that engages with domestic criminal law might invoke CDT principles, a cyber deterrence study that engages with laws of war between nation-states holds more resonance with SDT. In Jensen's SDT-influenced study of cyber deterrence, Jensen argues that prompt technical attribution remains an obstacle because *timely* attribution is necessary to mount a

counterstrike (2012, 798); otherwise, "the window to reasonably respond will be gone" (2012, 786).

By contrast, Will Goodman (2010) points to evidence from case studies in arguing that technical attribution is a theoretical problem that does not hinder cyber deterrence in actuality; the theoretical problem of technical attribution means that achieving cyber deterrence is "tougher in theory than in practice" (102). First, Goodman argues that the scope of the technical attribution problem is exaggerated; Goodman cites U.S. government agencies' success in technical attribution to prove that technical attribution is "not always the impossible challenge that some commentators make it out to be" (2010, 125). Second, Goodman points to the role of "assigned responsibility" in achieving cyber deterrence (108-109, 112-113). Goodman's study, which focuses exclusively on state-sponsored actors (105) suggests that international political blame can compensate for some deficiencies in technical attribution; thus, the technical attribution that serves as the basis for this international political blame need not be "definite" (125) so long as there is enough evidence to support the suspicion that the accused state-sponsored actors were the perpetrators of the cyberattack (128).

Goodman's emphasis on assignment of responsibility in cyber deterrence resonates with Jason Healey's seminal 2011 article "The Spectrum of National Responsibility for Cyberattacks." In this article, Healey acknowledged the role of technical attribution as a prerequisite for "cyberdefense" but argued that "perfect" technical attribution was not necessary for cyberdefensive actions between nation-states (2011, 57). Healey argued that it is assignments of state *responsibility*, rather than technical attributions themselves, that are required to mount "diplomatic, intelligence, military, and economic responses" (2011,

69); technical attribution therefore needed only to be of sufficient quality to be mobilized into supporting an assignment of state responsibility (2011, 57).

The U.S. seems to have used domestic criminal indictments as a means of so mobilizing technical attribution results. In a brief 2019 article, legal scholar Chimène I. Keitner identified and termed the "phenomenon" of "attribution by indictment" (207). Quoting Thomas Rid's and Ben Buchanan's argument that "[technical] attribution is what states make of it" (Rid and Buchanan 2015, 7), Keitner pointed out that the U.S. seemed to have developed a policy of using technical attribution results to issue criminal indictments that "implicate… foreign states in malicious cyber activity" (Keitner 2019, 207), thus assigning state responsibility. After identifying this phenomenon, Keitner's brief study – six pages in length – suggested policy implications for further research, among them the "deterrent function" of the U.S. indictments issued against foreign state actors (2019, 211). However, Keitner remained skeptical of whether these indictments could carry deterrent force. Despite evidence that Chinese cyberattacking activity declined after the 2014 issuance of the first U.S. indictment issued against suspected Chinese state-sponsored cyberattackers, Keitner's research had not yielded any study that established a causal link between the 2014 indictment and the decline, much less that deterrence was responsible: "Reports indicate that the raw volume of Chinese IP [intellectual property] and trade secret theft declined after 2014, but causation remains unclear. Declarations of success in deterring misconduct appear to have been premature" (Keitner 2019, 208).

To summarize scholarship on the extent of the problem of technical attribution, timely technical attribution may be theoretically necessary to mount counterstrikes under SDT-influenced models of cyber deterrence, but technical attribution does not seem to be

an insurmountable hurdle in cyber deterrence practice. When the deterrent action to be taken in response to a cyberattack is not an immediate counterstrike, but rather a "diplomatic, intelligence, military" or "economic" action (Healey 2011, 69), then technical attribution need not be immediate, and need only be of sufficient quality to support an assignment of state responsibility. The U.S. has mobilized technical attribution results to support assigning state responsibility via the issuance of domestic criminal indictments against alleged state-sponsored cyberattackers, but it is unclear whether – and if so, how – the indictments achieved a deterrent effect.

This project seeks to fill that gap in the literature by proving *that* the U.S.'s indictments have achieved deterrent effects against foreign cyberattacks both state and non-state, explaining *how* the U.S.'s indictments have achieved cyber deterrence, and elucidating *under what conditions* indictments can deter cyberattacks. To understand the theory on why bare indictments deter cyberattacks, an overview of criminal law and of indictments' place in American criminal procedure provides context.

2.3.1. Conceptualizing the criminal law

What is the criminal law? Legal philosophy and criminal sociology arrive at similar conceptualizations. Criminal laws are enacted by a society; crimes are offenses deemed unacceptable conduct from the perspective of that society as a whole (Duignan, n.d.). The criminal law can be contrasted with civil law; a civil harm – as opposed to a crime – is often traceable to a disagreement between private parties. To commit a civil harm is to commit an offense against a member of a society; to commit a crime, by contrast, is to commit an offense against the society (Duignan, n.d.). This conception of crime can be seen in criminal

law case names in American criminal law cases, where the 'person' bringing the case is ostensibly the society itself or all its members: in federal criminal law, "*United States of America v.* the criminal defendant"; at the provincial level, "*People v.* the criminal defendant," "*Commonwealth v.* the criminal defendant," or the like.

Likewise, in sociology, law is an expression of social norms. According to economists Roland Bénabou and Jean Tirole, the idea that the law "serves to convey a society's norms of behavior" is not only theorized, but also supported by historical empirical evidence that suggests that invoking the law can strengthen social norms or even establish them altogether (2011, 17). Supporting this conceptualization of the law as social norms, economists Daron Acemoglu and Matthew O. Jackson cite empirical evidence that "Laws often go unenforced when they conflict with prevailing social norms"; as the law is an expression of social norms, laws that are *not* aligned with social norms tend not to persist (2017, 246).

In classical CDT, administering the criminal law is a constitutive function – if not *the* constitutive function – of the state, as the criminal law stems from the state's duty to protect its members from harm. According to Beccaria, the state's imposition of criminal punishment was an obligation of the social contract (Beccaria 1764b, 8-11). Likewise, criminal law and the function of the state were inextricably intertwined in Bentham's writings, as criminal law was an integral component of what Bentham saw as the "business of government": "The business of government is to promote the happiness of the society, by punishing and rewarding. That part of its business which consists in punishing, is more particularly the subject of penal law" (Bentham [1789] 1823, 70). Moreover, the titles of the works in which Bentham's CDT principles appear evince the connection between

criminal law and the state; it is in Bentham's theory of *legislation*, and his treatise on morals and *legislation*, that his writings on CDT are to be found. Beccaria's and Bentham's conception of the state centered upon its function in administering criminal law. As criminal law is part of the "business of government," a state that did not administer the criminal law would arguably not be functioning as a state at all. For Beccaria and Bentham, statehood is defined by actions taken pursuant to the criminal law.

2.3.2. Indictments in American federal criminal procedure; extraditions; "bare" indictments

"Indictment" is a technical term. In American federal criminal procedure, an ***indictment*** is a type of criminal charge that is returned by a grand jury (Federal Bureau of Investigation, n.d.). A ***criminal charge*** is a formal accusation, issued by the state, that the person accused by the criminal charge has committed the crime specified in the criminal charge (Legal Information Institute, "Charge," 2022). Properly prepared criminal charges usually contain, in writing, what basis there is for the accusation; this is because criminal charges must be based on some evidence, or they would be 'baseless accusations' vulnerable to being invalidated. Besides indictment, another type of criminal charge in American federal criminal procedure is a ***criminal complaint***. A criminal complaint can be submitted to a federal court by a law enforcement official, and a criminal complaint is often used to issue an ***arrest warrant*** (see *Park Jin Hyok* criminal complaint). By contrast, an indictment is submitted to a federal court by a federal prosecutor. If the charged person is an individual rather than an entity, then arrest of that person can be made based on either an arrest warrant or an indictment (Federal Bureau of Investigation, n.d.). Federal criminal charges can be ***sealed***, also referred to as being issued under seal. A criminal charge's

being sealed means that its existence is kept unknown to the public and to the individual against whom it is issued (Federal Judicial Center 2009, 2). According to a 2009 report from the Federal Judicial Center, a frequent reason that criminal charges are issued under seal is to prevent the charged individual from being alerted to the risk of apprehension, as the charged individual may then be likely to take evasive action to avoid being apprehended (17-18). When a criminal charge is ***unsealed***, it becomes part of public record.

Procedurally, an important difference between criminal complaints and indictments is that before a federal prosecutor can submit an indictment, the indictment must be returned by a grand jury. The difference between criminal complaints and indictments is not a crucial distinction for understanding the theory on why bare indictments deter cyberattacks, as I will argue that the theory could be extended to domestic criminal charges generally, but this difference helps explain why U.S. federal charges against cyberattackers tend to be issued by indictment rather than by criminal complaint. The Fifth Amendment of the U.S. Constitution requires that federal prosecutions of "a capital, or otherwise infamous crime" be initiated by "indictment of a Grand Jury." If violating a federal criminal law is statutorily punishable by over one year of imprisonment (DOJ, "When an Indictment is Required," 2020), then violations of that federal criminal law constitute a "capital, or otherwise infamous crime." Violations of 18 U.S.C. § 1030, the U.S. federal criminal law against cyberattacks, are usually punishable by over one year of imprisonment. Therefore, prosecutions for alleged violations of this law must be initiated by "indictment of a Grand Jury," not by criminal complaint. Criminal complaints can still support an arrest warrant even if the crime specified is a "capital, or otherwise infamous crime," but even after an

individual is apprehended based on an outstanding arrest warrant, a prosecution of that individual for accused violations of such a "capital, or otherwise infamous" crime cannot lawfully commence unless and until an indictment is returned by the grand jury and submitted to the court by the prosecutor. After criminal charges are issued, a conviction can be accomplished either by a guilty verdict in a criminal trial based on those charges, or by a ***guilty plea***, in which the criminal defendant waives trial and formally admits that the criminal defendant has committed the crime with which the criminal defendant has been charged (see *Golestaneh* plea agreement).

From a U.S. perspective, ***extradition*** is when a foreign jurisdiction apprehends, or assists in apprehending, an individual against whom U.S. criminal charges have been issued and sends the individual from the foreign jurisdiction to the U.S. in order for the individual to face trial.[5] If the U.S. has a ***bilateral extradition treaty*** with the foreign jurisdiction, then the terms of the bilateral extradition treaty can legally obligate the foreign jurisdiction to make an extradition. However, if the U.S. does not have an extradition treaty with the foreign jurisdiction, then there is no legal obligation for the foreign jurisdiction to extradite individuals who have been criminally charged by the U.S. In addition, the laws of some nations prohibit the extradition of their own nationals (Harding 2007).

When there is no bilateral extradition treaty between the U.S. and the foreign jurisdiction against whose nationals the U.S. may issue an indictment, some analysts, scholars, and commentators see such 'bare' indictments as unlikely to result in conviction because there is no legal obligation for – indeed, there may even be a legal prohibition

[5] For further discussion of extradition, refer to the Council on Foreign Relations' explanation: "Extradition is the formal process of one state surrendering an individual to another state for prosecution or punishment for crimes committed in the requesting country's jurisdiction. It typically is enabled by a bilateral or multilateral treaty. Some states will extradite without a treaty, but those cases are rare" (Masters 2020).

against – the foreign jurisdiction's extradition of its own nationals to the U.S. Under U.S. law, a criminal trial cannot commence if the criminal defendant is not present to face trial (Koerner 2003). Therefore, when U.S. federal criminal charges are issued against a foreign national of a jurisdiction that does not have a bilateral extradition treaty with the U.S., some would argue that it is highly unlikely that the charged individual will ever face trial, much less be convicted (see Goldsmith 2014). This is what my project defines as "bare" indictments. ***Bare indictments*** are *indictments issued against foreign nationals of a jurisdiction that does not have a bilateral extradition treaty with the issuing jurisdiction.* Some examples of jurisdictions that currently are not party to an extradition treaty with the U.S. are China, North Korea, Iran, and Russia; therefore, indictments issued by the U.S. against nationals from any of these countries would be "bare" indictments.

2.4.1. Status, dominance, prestige, and face; common knowledge

Williams and Hawkins proposed that, for informal sanctions involving social disapproval to achieve an optimal deterrent effect, it must be established that the actor against whom those informal sanctions are to apply cares about the way that others in society view the actor. Can this premise be established when the actor is a nation-state? Indeed, scholars of international relations have proposed that concerns over place in a social hierarchy can predominate a nation-state's foreign affairs when the social hierarchy in question is the global order. This subsection first defines the interrelated sociological concepts of status, dominance, prestige, and face. Next, the subsection raises the role of common knowledge in affecting status. Then, this subsection gives a brief overview of how

status has been applied as a framework for explaining nation-state behavior in publicly observable events.

It should first be noted that the precise definitions of the sociological terms "status," "prestige," and "face" are themselves contested. For instance, Barry O'Neill (2006, 6) and Daniel Markey (1999, 128-129) have each noted that the definition of "prestige" is a subject of debate. Further complicating the matter is that since the terms refer to "closely related" concepts, the terms are often conflated (Ho 1976, 867-868).

For the purposes of this project, I will use the term ***status*** to mean *holding a high rank in a social hierarchy*. This definition of "status" resonates with the framework used by Deborah Welch Larson and Alexei Shevchenko in *Quest for Status: Chinese and Russian Foreign Policy*, which draws from social psychology for its conceptualization of status (2019, 3). Because this definition of status involves holding a high social rank relative to others, having status is a "positional good" dependent on making comparisons between one's own status and the status of other members of the society (Larson and Shevchenko 2019, 4).

There are multiple possible ways for an actor to achieve the goal of status. Since status is relative – whether one is highly ranked depends on how others are ranked in that social hierarchy – it follows that an actor might increase its rank by suppressing others' rank or by bolstering its own rank. Indeed, the "dual-strategies theory of social rank" (McClanahan et al. 2021, 2) posits that these multiple possible ways of making status gains fall into two essential categories: dominance and prestige. ***Dominance***, as discussed in this project, can be summarized as *asserting one's will over others in the social hierarchy and / or undermining others in the social hierarchy* (see Cheng and Tracy 2013; de Waal-Andrews et

al. 2015; Maner 2017; Cheng 2020). Meanwhile, I define gaining ***prestige*** as *obtaining or developing qualities or assets that one believes are admired by others in the social hierarchy* (see Cheng and Tracy 2013; de Waal-Andrews et al. 2015; Maner 2017; Cheng 2020). I will refer to these qualities or assets as ***markers of prestige***. Thus, dominance is a means of attaining high rank via lowering others' ranks, whereas prestige is a means of attaining high rank through raising one's own rank. Essentially, gaining prestige is moving up in the ranks by building oneself up; establishing dominance is moving up in the ranks by tearing others down. The two strategies share in common their aim to reach the same outcome; prestige-seeking and dominance-seeking are both means of attaining status.

Face, then, may be defined for this project as *one's outward expression of status* (see Ho 1976; Qi 2011). So defined, face might be comparable to one's 'public image.' For the members of the social hierarchy to assess the relative positioning of a given member – whether themself or another – there must be some observable information relating to dominance and prestige. In demonstrating dominance, the mere fact of asserting one's will over another does not in itself mean one will be acknowledged and treated as having high rank; besides the possibility of this assertion being taken poorly by the other members of the social hierarchy, the other members could not use the fact of an actor's dominance to evaluate status if the fact of the actor's dominance is unknown to them. Likewise, the mere fact of obtaining a marker of prestige will do nothing to increase status if the fact is not made known to others. Besides the possibility that the other members of the social hierarchy may not in actuality find the marker of prestige to be admirable, the other members could not use the fact of an actor's prestige to evaluate status if the fact of the actor's prestige is unknown to them. Given that status is relative, judgments about status

are based on the information known about other members of the social hierarchy. As discussed in this project, "face" has a connotation of intentionality: face refers to information, relevant to status, that an actor *wants* known about itself.

Conceptually, then, a member's self-assessment of its own relative rank is dependent on one's *beliefs* regarding what information about it is known to the other members; thus, O'Neill (2006) posits that the distribution of information that can garner prestige is most effectively achieved by ***common knowledge*** (13). Common knowledge, as explored by Michael S. Chwe's 2001 book *Rational Ritual*, means not only that one knows a piece of information, but also that one knows that this piece of information is known by the other members of the society: "knowledge of the message is not enough; what is also required is knowledge of others' knowledge, knowledge of others' knowledge of others' knowledge, and so on – that is, 'common knowledge'" (Chwe 2001, 3). As both Chwe and O'Neill underscore, events that make a piece of information publicly known make this information common knowledge (Chwe 2001, 3-4; O'Neill 2006, 13). When a piece of information becomes publicly released and hence common knowledge, every member has a strong basis for believing that the information is known to the other members and that the information can therefore be factored into each member's status assessments.

International relations studies have yielded empirical evidence that nation-states seek status (Renshon 2016, 522-523), with the "social hierarchy" in a world politics context being the international community. According to Jonathan Renshon's 2017 book *Fighting for Status: Hierarchy and Conflict in World Politics* as well as Renshon's 2016 article "Status Deficits and War," status-seeking has even been a reason behind state initiation of interstate wars (Renshon 2017; Renshon 2016, 526), as wars are public events visible to all

members of the international community. Under the definitions used in this project, a nation-state's intentional initiation of a war with another nation-state can be seen as a face-generating event. Given that common knowledge is generated by publicization, Larson and Shevchenko in *Quest for Status* argue that status-seeking (2019, 3-4) explains nation-state behavior when a nation-state not only has seized an asset that can be construed as a marker of prestige, but also seeks to publicize its seizure and holding of that asset to other members of the international community (2019, 234-235). Larson and Shevchenko use the example of capturing additional territory, which could be considered dominance-seeking, prestige-seeking, or both; the action of seizing land from rival nation-states is an example of asserting one's will over others, and the land itself might be seen as an admired asset. The authors use case studies from China and Russia to show that status-seeking was a predominant concern for these nation-states' behavior in prioritizing geographic expansion: "if they were solely interested in the economic benefits to be derived from expansion, Chinese and Russian rulers would not have been so concerned about publicizing their victories" (Larson and Shevchenko 2019, 235).

Even though some may dispute that prestige as a concept confers any benefits, it is difficult to dispute that nation-states are frequently concerned with prestige-seeking. For instance, Jonathan Mercer's counterargument that state prestige-seeking is an "illusion" centers on contentions that the strategy of state prestige-seeking is, in effect, difficult to measure and unlikely to succeed (Mercer 2017, 134); Mercer acknowledges, however, "The evidence that states seek international prestige is overwhelming" (133). In short, it is nearly indisputable that many nation-states care about face, and that they engage in status-seeking via prestige-seeking or dominance-seeking activities.

2.4.2. Attribution theory and respondeat superior

Attribution theory, another framework drawn from social psychology, regards how assignments of causation, responsibility, and blame are made (Fincham and Jaspars 1980). For the purposes of this paper, it is necessary to understand one principle of attribution theory: the principle of imputing responsibility from a subordinate to a superior in a hierarchy. V. Lee Hamilton's 1986 study "Chains of Command: Responsibility Attribution in Hierarchies" identifies the condition necessary for any viewer to impute to the superior responsibility for a subordinate's misconduct: when it is perceived that the superior could have and should have done something to prevent the subordinate's misconduct, then blame and responsibility for that misconduct may be imputed to the superior (120). This perception is likely to be held whenever the superior-subordinate relationship is made clear, since oversight over a subordinate's actions is an expected part of a role as a superior (Hamilton 1986, 120). Thus, whenever it is made known that an agent was acting under a superior's oversight – even when it is not clear whether the agent was acting under express orders from the superior – responsibility for misconduct committed by the agent is likely to be assigned to the superior.

Hamilton notes that this principle of attribution theory, which is predictive of beliefs held in the minds of viewers, coincides with the principle of *respondeat superior* for legal liability. ***Respondeat superior*** means "let the superior be answerable for the misconduct of the subordinate"; according to international law scholar Gary D. Solis, *respondeat superior* means that "the commander is criminally responsible, but did not actually order the wrongful act done… although there was no order, the commander is responsible

because… [the commander] initiated or acquiesced in the wrongdoing, or took no corrective action upon learning of it" (Solis 2010, 381). The perceptual condition necessary for *respondeat superior* to apply can be summarized thusly: *respondeat superior* applies when it is established that the superior had some level of control over the subordinate's misconduct, yet failed to exercise this control to stop the misconduct.

The superior's imputed responsibility is not necessarily all-or-nothing; imputed responsibility can be gradated. The experiment described in Hamilton's paper conceives of different extents of imputed responsibility, which are roughly representable by percentages (1986, 125). Thus, the extent to which the superior is legally liable for the subordinate's misconduct can vary.

The next chapter will integrate the concept of common knowledge with the role of publicization in CDT to show how bare indictments – in accordance with attribution theory and *respondeat superior* – can deter by triggering informal sanctions that include attacks on face, which are imputable against states.

CHAPTER 3

STUDY DESIGN:

THEORY, DATA, AND HYPOTHESES

3.0. Hypotheses and Predictions; Introduction to the Study Design

Whether a bare indictment will serve as an effective deterrent measure against future cyberattacks depends on the motives of the alleged cyberattacker against whom the bare indictment was issued. This chapter covers the theory, data, predictions, and methodology that will be utilized in proving this contention. My project argues that the deterrent effects of bare indictment hinge upon the role of the package of informal sanctions that bare indictment triggers. I theorize that the package of informal sanctions triggered by bare indictments' labeling the accused cyberattacker a "criminal outcast" directly undermines status-seeking objectives and indirectly outweighs thrill-seeking objectives, but neither directly undermines nor indirectly outweighs profit-seeking objectives.

Thus, the central super-hypothesis is that bare indictments are likely to deter cyberattacks that are primarily motivated by status-seeking and / or thrill-seeking, but bare indictments are less likely to deter cyberattacks that are primarily motivated by profit-seeking. Referring to the variables in the deterrence inequality $(P_C)(C) > (P_B)(B)$, this super-hypothesis can be broken into three hypotheses:

- **H1**: Bare indictments are likely to deter status-seeking cyberattacks, because the attack on face in the package of informal sanctions triggered by bare indictment

tends to directly undermine the adversary's expected benefit of status; these informal sanctions can lower *B* such that $(P_C)(C)$ is likely to exceed $(P_B)(B)$.

- **H2**: Bare indictments are likely to deter thrill-seeking cyberattacks, because the practical consequences in the package of informal sanctions triggered by bare indictment tend to indirectly outweigh the adversary's expected benefit of emotional thrill; these informal sanctions can raise P_C and / or raise *C* such that $(P_C)(C)$ is likely to exceed $(P_B)(B)$.
- **H3**: Bare indictments are unlikely to deter profit-seeking cyberattacks, because the package of informal sanctions triggered by bare indictment is neither likely to directly undermine nor likely to indirectly outweigh the adversary's expected benefit of monetary profit.

In short, this project hypothesizes that a cyberattacker's motives, as evidenced by the cyberattacker's behavior, are the determinants of bare indictments' deterrent effect. I also suggest a fourth hypothesis:

- **H4**: The deterrent effect of a bare indictment issued against an alleged cyberattacker will tend to be applicable against that alleged cyberattacker's foreign nation-state in accordance with the principle of *respondeat superior*.

Notice that the wording of **H4** concerns the deterrent effect's *applicability* against the foreign national's nation-state, rather than whether the deterrent effect will actually *deter* this nation-state. This means that any bare indictment issued against an alleged cyberattacker, however that alleged cyberattacker was motivated, will tend to be applicable against the alleged cyberattacker's nation-state if it can be established that the

nation-state had some level of control over the cyberattack, yet the nation-state evidently – because the cyberattack at issue in the bare indictment was actually executed – failed to exercise its control to stop the cyberattack. Whether this imputed deterrent effect will actually deter the nation-state depends, in turn, on whether the informal sanctions would directly undermine and / or indirectly outweigh the nation-state's objectives. Those national objectives may or may not be aligned with the alleged cyberattacker's motives.

Relatedly, a fifth hypothesis is as follows:

- **H5**: Given that many nation-states care about national status, nation-states against whom bare indictments are imputable will be sensitive to the applicable deterrent effects of the "criminal naming-and-shaming" attack on face that bare indictments achieve.

The sixth hypothesis is based upon the combined mechanistic influence of the other hypotheses, as it is premised on the assumption that bare indictments will indeed achieve deterrent effects against status-seeking and thrill-seeking:

- **H6**: When bare indictments are issued against suspected cyberattackers and publicized, then over time cyberattacks will shift toward being motivated by profit-seeking.

If bare indictments deter cyberattacks that are primarily motivated by status-seeking and / or thrill-seeking, then cyberattacks so motivated would be less likely to be perpetrated. Therefore, over time, almost all cyberattacks would come to be motivated by profit-seeking.

These six hypotheses yield six predictions corresponding to each respective hypothesis:

- **P1**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by status-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.
- **P2**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by thrill-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.
- **P3**: No indicia of deterrent effects will likely be observable after the publicization of a bare indictment issued against an alleged cyberattacker primarily motivated by profit-seeking.
- **P4**: Even though the nation-state itself is not a named defendant, the nation-state government may issue an indignant public statement in response to a bare indictment of individuals alleged to be cyberattacking on the nation-state's behalf.
- **P5**: When a publicized bare indictment is applicable against a nation-state that cares about national status, the nation-state will likely react by attempting to recover status.
- **P6**: Over time, publicized bare indictments will come to be issued almost exclusively against cyberattacks that are motivated by profit-seeking.

These predictions' emphasis on "publicization" is due to the deterrence theory principle that the deterrent measure must be known to the potential adversary. In

accordance with classical CDT's precept that the existence of a deterrent measure cannot be kept unknown, issuance of a bare indictment cannot achieve deterrent effects if the indictment is under seal.

To test this theory, I use case studies of publicized U.S. bare indictments that were issued against alleged cyberattackers. I select bare indictments that allege violations of 18 U.S.C. § 1030, which is an American federal statutory criminal law that coincides with this project's definition of "cyberattack." A dataset compiled by Trevor Logan and Pavak Patel from the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies suggested many case studies that fit these criteria. I cleaned, consolidated, and supplemented the data in this dataset to arrive at a list of fifty bare indictments that allege violations of 18 U.S.C. § 1030; I then consolidated these bare indictments into twenty-seven case studies whose publicization dates span from January 2012 to March 2022. A before-and-after study design centering on the case studies is used, wherein a sudden stop or sharp decline in cyberattacking activity is the strongest indication of deterrent effects; as for causation, there is a convincing inference that the bare indictment caused the deterrent effects when this sudden stop or sharp decline occurs shortly after the publicization of the bare indictment. Causation is further proven by ruling out competing explanations for the deterrent effects.

The remainder of this chapter is organized as follows. Section 3.1. and Section 3.2. discuss the theoretical mechanisms underlying the hypotheses. Section 3.1. focuses on **H1**, **H2**, and **H3** by discussing the respective effects that the package of informal sanctions triggered by bare indictment would have upon the three different motives of status-

seeking, thrill-seeking, and profit-seeking. Status-seeking is divisible into prestige-seeking and dominance-seeking, but I theorize that the mechanistic effects are similar across the prestige-seeking and dominance-seeking motives because informal sanctions are a denial of status. Section 3.2. discusses how to analyze behavior to determine motive, and Section 3.2. provides a table regarding indicators of a cyberattack's motive. Then, Section 3.3. focuses on discussion of **H4** and **H5**; to give a basis for hypothesizing that nation-states can be deterred at all by bare indictment and that many nation-states will be sensitive to an accusation of criminality, I place theoretical principles of imputed responsibility in dialogue with theories on attacks to face and theories on the process of criminalization. Section 3.4. provides a foundation for **H5** by theorizing a shift to profit-seeking. In Section 3.5., I discuss the before-and-after study design. This section also covers the types of evidence used; I refer to the publicly released text of the indictment and to publicly available news articles on the cyberattacks allegedly perpetrated by those individuals. To show evidence of whether bare indictments achieved a deterrent effect, I refer to publicized governmental statements and to publicly released technical attribution reports from cybersecurity researchers. Section 3.6. covers case study selection, analyzing 18 U.S.C. § 1030 to show why this law is well suited as a case selection criterion. Serving as an illustrative example of how datasets may be cleaned to aid in constructing small-*N* qualitative studies, descriptions of the available data and a step-by-step description of the data cleaning process are covered in Section 3.7., which culminates in an original dataset of the case studies. Finally, Section 3.8. concludes Chapter 3 by covering the organization of the remaining chapters in the study and giving a table that summarizes the hypotheses and predictions.

3.1.0. Theorizing The Package of Informal Sanctions and The Three Common Motives of Cyberattackers

I hypothesize that bare indictments, or other domestic criminal charges, are likely to deter cyberattacks when they are issued against actors who are primarily motivated by status-seeking or thrill-seeking. Bare indictments or other domestic criminal charges are less likely to deter cyberattacks when they are issued against actors who are primarily motivated by profit-seeking. In accordance with this typology of three common motivations for cyberattackers, bare indictments' deterrent effect upon actors who are better characterized as having mixed motives is dependent on whether one of the motives is profit-seeking. That is to say, bare indictments will be likely to deter actors who have mixed thrill-seeking and status-seeking motives; meanwhile, bare indictments will be unlikely to deter actors who have mixed profit-seeking and thrill-seeking motives, and bare indictments will likewise be unlikely to deter actors who have mixed profit-seeking and status-seeking motives.

Thus, this section provides the theoretical foundation for hypotheses **H1**, **H2**, and **H3**:

- **H1**: Bare indictments are likely to deter status-seeking cyberattacks, because the attack on face in the package of informal sanctions triggered by bare indictment tends to directly undermine the adversary's expected benefit of status; these informal sanctions can lower *B* such that $(P_C)(C)$ is likely to exceed $(P_B)(B)$.

- **H2**: Bare indictments are likely to deter thrill-seeking cyberattacks, because the practical consequences in the package of informal sanctions triggered by bare indictment tend to indirectly outweigh the adversary's expected benefit of emotional thrill; these informal sanctions can raise P_C and / or raise C such that $(P_C)(C)$ is likely to exceed $(P_B)(B)$.
- **H3**: Bare indictments are unlikely to deter profit-seeking cyberattacks, because the package of informal sanctions triggered by bare indictment is neither likely to directly undermine nor likely to indirectly outweigh the adversary's expected benefit of monetary profit.

This section conceptualizes bare indictments as a package of informal sanctions whose deployment is triggered upon the bare indictment's publicization, an action that labels the accused cyberattacker a criminal outcast. Section 3.1.1. analogizes bare indictments – and their publicization – to CDT principles regarding apprehension probability and optimal deterrence. Section 3.1.2. discusses sociological literature on the process of criminalization to explain why the outcasting effect is incompatible with status and hence is highly detrimental to face. Next, Section 3.1.3. extrapolates from the literature on common knowledge to show why an attack to face is most effectively achieved through making information common knowledge. Section 3.1.4. theorizes the components of the package of informal sanctions. Section 3.1.5. presents the common motives of cyberattackers and discusses informal sanctions' interaction with each motive. A table summarizing the predicted deterrent effects of informal sanctions upon each motivation concludes the section. These predictions, again, are as follows:

- **P1**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by status-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.
- **P2**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by thrill-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.
- **P3**: No indicia of deterrent effects will likely be observable after the publicization of a bare indictment issued against an alleged cyberattacker primarily motivated by profit-seeking.

3.1.1. The Features of Bare Indictments Resonate with CDT Principles

A recapitulation of four CDT principles helps contextualize the core theory on bare indictments. First, potential offenders tend to be deterred by the probability of apprehension. Some CDT scholarship posits that the probability of apprehension, rather than the probability of conviction, is dispositive in achieving the deterrent effect because it is apprehension, as distinct from conviction, that triggers informal sanctions. This theoretical prediction is empirically validated by criminologist Daniel S. Nagin's meta-analysis (2013), and Mark D. West's study suggests that the informal sanctions that apprehension triggers are responsible for the deterrent effect of apprehension (2003).

Second, informal sanctions are thought to be determinative of the deterrent effect. As discussed in Chapter 2, some CDT literature suggests that informal sanctions, rather than formal legal consequences, are mainly responsible for achieving criminal deterrence.

It is mainly the expectation of informal sanctions, rather than the expectation of formal legal consequences, that tends to deter potential offenders from committing crimes.

Third, actual imposition of a punishment upon a person who has committed the offense to be deterred achieves general and specific deterrence going forward. In the event of specific deterrence failures, classical CDT theorizes that the way general deterrence is made credible is by the actual imposition of the punishment. Classical CDT theorizes that members of the public, seeing that a person who committed a certain offense was then punished for that offense, may then be deterred from committing that offense because they can expect that they too will be punished for committing that offense. This is the general deterrent effect. Given that the punishment is imposed on the person who committed that offense, classical CDT also predicts that the imposition of punishment also achieves a specific deterrent effect against the person upon whom it is imposed. This is because classical CDT posits that the person will expect to again be punished if the person commits a recidivist offense.

Fourth, publicization optimizes criminal deterrence. To achieve an optimal deterrent effect, the imposition of the punishment cannot be kept secret from the public. If the public were prevented from knowing about the imposition of the punishment, then the deterrent effect would be suboptimal; deterrent measures can only deter if they are known to a potential offender. If the only potential offenders who know about the imposition of a punishment are the original offender and the state agents who are administering the punishment, then the deterrent effect will be limited to those few persons. By contrast, many more potential offenders could have been deterred and the general deterrent effect

could have been optimized were the punishment known – or made known – to the public. There is no guarantee that the knowledge of the punishment's imposition will achieve a general deterrent effect, but when the imposition of punishment is kept unknown, then there is *zero* chance that the punishment's imposition – as opposed to some external, intervening cause – can achieve a general deterrent effect.

Building upon these four CDT principles, it can be clarified why indictments, or other forms of domestic criminal charges, may be theorized to deter potential cyberattackers from committing cyberattacks. Amidst the remote operations of the cyber context, being criminally charged from afar is comparable to being physically apprehended; like apprehension, the imposition of criminal charges triggers informal sanctions. This trigger occurs because indictments formalize the results of technical attribution, just as an apprehension formalizes the findings of a traditional criminal investigation. Apprehension reveals the existence of the accused individual's actions, categorizes those actions as criminal, portrays the accused individual as the suspected perpetrator of those crimes, and therefore labels the accused individual a suspected criminal offender. Making that apprehension – the imposition of punishment – publicly known is instrumental in engendering social disapproval. The public may have already known about the accused individual's actions, and may even know that the accused individual is the perpetrator of those crimes, but apprehension makes it common knowledge that those actions have been officially deemed criminal, and also makes it common knowledge that the state has reason to believe that the accused individual is the suspected perpetrator. Bare indictments – even in the absence of formal arrest, trial, and conviction – accomplish the same functions

as do apprehensions. By analogy, then, bare indictments may be predicted to trigger informal sanctions that can achieve a deterrent effect.

3.1.2. Apprehension as Criminalization and Social Outcasting

Even though apprehensions are reflective of suspicions rather than of legal determinations of criminal liability, in effect the apprehension labels the accused individual a "criminal outcast" from a societal perspective. Being apprehended is not a legal determination that the apprehended person has committed that crime, yet empirical evidence shows that apprehension nevertheless plays the dispositive role in criminal deterrence. Why might being labeled a criminal outcast act as such a strong deterrent? Looking to theories on criminalization suggests that apprehensions – a form of contact with the criminal justice system – contribute to a process that gradually ousts the individual from membership in society and hence removes any status the individual may have held.

Sociologically, the process of criminalization can be considered a process of social outcasting in which the label of "criminal," iteratively applied by the individual's being subject to the governmental criminal justice process (Little 2006, 296), gradually strips the 'criminal' deviant individual of the individual's status in the mainstream social hierarchy (Medina Falzone 2021). Constructivist sociological theories posit that since crime is an expression of social norms, it is not necessarily the inherent wrongness of an action that leads to outcasting; rather, committing those actions *that have been deemed crimes* from

the perspective of a certain society demonstrates the actor's deviance from social norms and can therefore lead to social disapproval (Rosenfeld 2009).[6]

Although "the same behavior may be considered criminal in one society and an act of honor in another society or in the same society at a different time" (Rosenfeld 2009), if one assumes that an action *has already been deemed a crime* rather than an act of honor and the law criminalizing such action is aligned enough with social norms against that action that the law is not in danger of dying out, then the revelation of a given actor as the perpetrator of that criminal action portrays the actor as a social deviant (Little 2006, 294). Conceptually, then, one cannot hold a high rank in a social hierarchy if one is not considered a member of that social hierarchy at all.

A possible objection to this conclusion would be to raise the possibility that criminality can be a means of gaining status in society. However, theories of criminality that regard the development of "criminal subculture" suggest that the only 'high rank in a social hierarchy' one is likely to gain from being criminalized is not a high rank in the society that has criminalized one's actions, but rather, a high rank in a hierarchy made up of other social outcasts (Matsueda et al. 1992). As mentioned above, it is not necessarily that the 'criminal' act at issue is inherently wrong. Rather, it is that the act has been deemed wrongful from the perspective of that society. Hence, unless the underlying societal norms

[6] Interestingly, some scholars have presented this theorized process of criminalization – sometimes referred to as ***labeling theory*** (Little 2006, 296; Thomas and Bishop 1984, 1225) – as a competing theory to CDT, since these scholars posit that the respective principles of these two theories yield contrasting predictions (Ward and Tittle 1993, 44-45; Thomas and Bishop 1984, 1225). I would argue that labeling theory and CDT are not as incompatible as some scholars would make them out to be. It seems that a main point of contention between labeling theory and CDT rests on the argument that labeling theory works via the labeled individual's *self-perception* as a criminal outcast (Ward and Tittle 1993, 43-45). My theory on bare indictments does not hinge on self-perception, but rather, on the perception of others in the social hierarchy. This distinction, if empirically true, would not change the criminalization process described by labeling theorists; however, the mechanism by which this process operates – self-perception versus social perception – would be different. In short, I would theorize that the label of "criminal outcast" can be a deterrent.

about whether that act is wrongful change, the label of "criminal outcast" is incompatible with holding *any* rank in that social hierarchy, much less a *high* rank in that social hierarchy.

In short, criminalization is conceptually incompatible with status. Every instance of being subject to the governmental justice system – such as by being indicted, which is one way of being formally accused of a crime – represents an attack to status. This attack's deployment is triggered upon publicization.

Criminalization is theorized to be a process, so repeated impositions of the "criminal outcast" label can be additive rather than all-or-nothing. A 'criminal' has already been outcasted from the mainstream social hierarchy to a certain degree; one's high rank in a social hierarchy is insecure if one's membership in that social hierarchy is itself tenuous. Someone who gradually becomes a social outcast cannot simultaneously be maintaining a high status in a social hierarchy; likewise, social disapproval is the polar opposite of being viewed favorably by most other members of society.

If bare indictments can be analogized to apprehensions – which deter by triggering informal sanctions – then, correspondingly, being indicted or otherwise criminally charged may deter by triggering informal sanctions. If the "punishment" here is conceptualized as the package of informal sanctions that labels the suspected cyberattacker a "criminal outcast," then the punishment is imposed when the criminal charges are issued *and made known to the public*. Criminal charges under U.S. law can, as discussed in Chapter 2, be kept under seal; thus, the stage at which bare indictments can be predicted to achieve both general and specific deterrence is when they are made known to the public.

It is not the knowledge that an individual has committed an act, but rather the knowledge that this individual has committed a *criminal* act, that attacks the individual's face, hence directly undermining status-seeking. This concept will be further addressed in Chapter 4's discussion of the distinction between *criminal* shaming and other forms of social shaming.

Given that criminal law is an expression of social norms, and a violation of a crime is seen as an offense against all society's members, it can be observed that criminal misconduct would be especially destructive to status if the misconduct – more importantly, its criminality – is not only made known to all members of the society individually, but is also made common knowledge.

3.1.3. Publicization of Bare Indictments Makes Attacks on Face Common Knowledge

Here, publicization of the punishment's imposition is not only crucial for optimizing deterrence – as CDT predicts that publicization is always necessary to optimize deterrence for all forms of state-imposed "punishment" – but also plays an integral role in the functioning of the deterrent effect itself when the punishment is the package of informal sanctions. This is because one of the components of the package of informal sanctions is an attack on face. As discussed in Chapter 2, face is the outward expression of status, and status is a relational concept regarding one's high rank in a social hierarchy. Because status is relative, whether one believes one holds high status is dependent on one's estimation of others' views. Common knowledge means that all members of a group not only know a piece of information, but also know that the piece of information is known to all other members.

The theories discussed in Chapter 2 predict that common knowledge is a means of affecting prestige, for better or worse. Making a victory common knowledge is theorized to be an effective – or, some scholars would argue, a necessary (O'Neill 2006, 13) – way to increase prestige; if publicization is an effective or necessary way to bolster status, publicization might also be an effective or necessary way to attack status. Publicly communicating to all members of the society that one of its members has committed an action that is inconsistent with what the society conceives of as high rank should make it known to every member – including, most importantly, the member who is being attacked – that the attack on face is known to the other members. Especially when the information communicated in the attack on face would be difficult to dispute – that is to say, the underlying information mobilized in the attack on face is readily verifiable – every member is likely to believe that other members are unlikely to view the attacked member favorably.

Because a crucial component of the package of informal sanctions is an attack on face, publicization of indictment optimizes informal sanctions' deterrent effect by making this attack on face common knowledge.

3.1.4. Components of the Package of Informal Sanctions

What, then, are the components of the package of informal sanctions that indictment triggers? I theorize three components, two of which are relevant to this study. All three relate to an indictment's labeling the suspected cyberattacker a "criminal outcast." These three components are

- an attack on status,

- internal negative feelings, and
- practical consequences.

One component is, as mentioned, an attack on status, which could alternately be phrased as an attack to face. Criminological literature suggests that being viewed in society as a "criminal outcast" is inherently incompatible with holding a high status in that social hierarchy. Other members of society may already view a suspected cyberattacker as a "cyberattacker" or even an "offender," meaning that the suspected cyberattacker already may be seen as having deviated from societal norms, but being labeled a "criminal" makes the suspected offender the worst kind of social deviant: the sort who has broken the norms that are enshrined in law, and hence has perpetrated an offense against the society itself. The label of "criminal outcast" carries little weight if it is thrown around as an insult between private parties, since a private party does not have the state's authority to declare that someone is a criminal. Criminal indictment, by carrying the state's authority to administer the criminal law on behalf of the members of that society, convincingly imposes the label of "criminal outcast" and hence attacks the alleged cyberattacker's status. Because a bare indictment can be analogized to an apprehension in the process of criminalization, one of the informal sanctions is an attack on face.

I refer to this component as, alternately, an 'attack on status,' which is a denial of rank; or an 'attack to face,' which is an undermining of the outward expression of that rank. Note that this is distinct from an 'attack to prestige.' A label of criminality does not necessarily take away one's ownership of markers of prestige, nor does labeling someone a "criminal outcast" necessarily denigrate their prestige assets. The component attacks the

outcome of status, not the *path* by which status is garnered. As mentioned in Chapter 2, the two paths by which status can be sought are prestige and dominance. Hence, this terminological distinction is important because a component that denies the outcome of status rather than hinders the path of prestige would – in theory – attack both dominance-based status and prestige-based status.

The second component – upon which my study does not focus – regards internal negative feelings of shame and guilt that may result from being labeled a "criminal outcast." It is worth mentioning that this could be one of the components of the package of informal sanctions, but my study does not cover any case in which these internal feelings were determinative of the deterrent effect in an individual.[7] This may be because it can usually be assumed that cyberattackers are often 'shameless'; even cyberattackers motivated by emotional thrill-seeking – which is further discussed in the next subsection – may derive their emotional thrill from the knowledge that they are breaking the law, so simply affirming this knowledge is unlikely to 'guilt' or 'shame' cyberattackers into being deterred. Also, conceptually, *internal* feelings of shame and guilt are not as readily perceivable by *external* observers, so the general deterrent effect of internal feelings will probably be limited because publicization of the informal sanctions' imposition does nothing to render the accused's internal feelings directly observable. Accused cyberattackers who are fugitives from justice presumably would not be personally making public appearances to

[7] My study does conduct an in-depth case study of a case in which 'humiliation' or something akin to it is thought to have deterred a state rather than an individual, but this humiliation is better conceptualized as part of the attack on status because – as discussed in that case study, which is the U.S. Financial Industry DDoS attacks case study – humiliation is, like status, a relational concept. One way to conceptualize humiliation is as the result of a denial of status, since humiliation involves the "public failure" of a "status claim" (Torres and Bergner 2010).

make their shame and guilt common knowledge by speaking about their internal negative feelings, so any general deterrent effect of this component is suboptimal and insignificant.

The third component is the practical consequences that come with being labeled a "criminal." These practical consequences are the risk of apprehension and the risk that formal legal consequences will apply. Being apprehended would, in turn, trigger another package of informal sanctions, the expectation of which the CDT literature theorizes is responsible for criminal offenders' being deterred by the probability of apprehension. When criminal charges are made public, they become known to the indicted actor; thus, publicizing the label of "criminal" helps impart the probability of apprehension upon the cost-benefit calculus of the indicted actor. Thus, given that CDT posits that the probability of apprehension is responsible for the deterrent effect, one reason that indictments can deter is raising the probability of apprehension to a significant risk; publicization makes this risk known to the accused cyberattacker, such that the accused cyberattacker can factor this risk into expected weighted cost. If the expected weighted cost outweighs the expected weighted benefit such that the accused cyberattacker is convinced that avoidance of apprehension should take precedence, this component can have a deterrent effect upon cyberattacks by making the accused cyberattacker refrain from conducting cyberattacks that could call more attention, reveal the accused cyberattacker's position, and lead to the accused cyberattacker's arrest.

///

///

3.1.5. Common Motives of Cyberattackers; Informal Sanctions' Interaction with Motives

To understand the reason why the difference in deterrent effect is theorized to be dependent on motive, it is first necessary to have a conceptual understanding of each of the three common motives of cyberattackers: **status-seeking**, **thrill-seeking**, and **profit-seeking**. Status-seeking can be accomplished by either of two paths – **prestige-seeking** and **dominance-seeking** – so the full list is as follows:

- Status-seeking
    - via Prestige-seeking
    - via Dominance-seeking
- Thrill-seeking
- Profit-seeking

In accordance with the concept of "prestige," this paper defines **status-seeking** as having the objective of raising one's rank in the mainstream social hierarchy. This aim can be reached via **prestige-seeking**, rising through the ranks by obtaining assets that one sees as markers of prestige; or via **dominance-seeking**, asserting one's will to suppress the rank of others. Both prestige-seeking and dominance-seeking are types of status-seeking. For the purposes of this paper, **thrill-seeking** means having the objective of gaining positive emotions. Criminological literature posits that gaining positive emotions in the criminal context is usually accomplished by executing actions – namely, criminal offenses – that one sees as exciting (Burt and Simons 2013). I conceptualize thrill-seeking as the weakest motive, as it can be used to characterize cyberattackers who seem to execute cyberattacks for no apparent reason. **Profit-seeking**, as defined by this paper, means

having the objective of obtaining monetary or otherwise economic benefits. A taking of currency would be an example of profit-seeking. In the cyber context, data is a valuable commodity, so any taking of data can also be an indication of profit-seeking. Thus, whenever cyberattacks involve a taking of currency or a taking of data, the baseline assumption on motive can be that those cyberattacks are primarily motivated by profit-seeking.

By respectively plugging these three motives in as the variable of expected benefit in the cyberattacker's cost-benefit calculus, it can be observed that the informal sanctions tend to directly deny the expected benefit of status and indirectly outweigh the expected benefit of thrill. For primarily status-seeking cyberattackers, the expected benefit is status. A component of the package of informal sanctions that is triggered by indictment is an attack on status, as the indictment labels the offender a "criminal outcast." Since an attack on status would deny the expected benefit of status, this component of a bare indictment's informal sanctions package deters prestige-seeking cyberattacks by lowering the expected benefit of their alleged perpetrators.

For primarily thrill-seeking cyberattackers, the expected benefit is emotional thrill. A component of the package of informal sanctions triggered by indictment is practical consequences, particularly the risk of apprehension. It is predicted that the expected weighted cost of these practical consequences will often be sufficient to outweigh the expected benefit of emotional thrill; indictments label the indicted thrill-seeking actor a "criminal outcast" and hence a fugitive from justice. For this reason, the indicted thrill-seeking actor is likely to become preoccupied with avoiding apprehension. In accordance

with CDT studies, the probability of apprehension is predicted to exert a psychological cost. Moreover, it is predicted that the indicted actor who wants to avoid apprehension will then 'keep a low profile' and avoid taking any actions that would reveal the indicted actor's location, since this could lead to apprehension. Mounting a recidivist cyberattack is an example of an act that could call attention to the indicted actor's location; after the risk of apprehension is imposed, thrill-seeking cyberattackers are likely to be deterred from recidivist cyberattacks since they are likely to be convinced that the expected weighted cost is too high.

With practical consequences increasing expected weighted cost, the informal sanction of bare indictments' practical consequences can be predicted to deter thrill-seeking cyberattacks by raising the expected weighted cost of their alleged perpetrators such that expected weighted cost exceeds expected weighted benefit. It might be useful to conceptualize practical consequences as tending to raise the expected probability of cost, the expected cost, or both. The risk of apprehension raises the expected probability of cost, since a cyberattacker might already have contemplated the cost of being arrested yet may expect a very low probability of being arrested. Practical consequences can also raise, or at least affirm, a cyberattacker's expected costs such as the psychological costs of being arrested or the cost of being subject to *formal* sanctions; prior to knowing about the indictment issued against them, cyberattackers may be less likely to contemplate the costs that would apply upon apprehension. Procedurally, since an indictment enables arrest, the practical consequences in the package of informal sanctions legitimate the possibility of arrest and make an arrest more likely. As mentioned, the probability of apprehension tends to be a potential offender's P_C. Thus, the practical consequences in the package of

informal sanctions can effectuate both a raise in P_C, expected probability of apprehension; and a raise in C, expected costs that would be triggered upon apprehension. Either or both of these directions will tend to raise expected weighted cost such that it exceeds the expected weighted benefit for cyberattacker whose objective is to gain emotional thrill.

By contrast, if the cyberattack is primarily motivated by profit-seeking, informal sanctions are unlikely to have any deterrent effect. Unlike with status-seeking, informal sanctions do not lower the expected benefit B of economic profit. The imposition of formal punishment – such as a monetary fine or jail time – might have an effect on directly denying economic profit, but no component of the package of informal sanctions directly denies monetary profit. It may be true that the practical consequences do raise P_C and C to a certain extent, but this raise will probably be comparatively insignificant and hence negligible; assorted practical consequences including the risk of apprehension are unlikely to make the expected weighted cost exceed the expected weighted benefit when a typical profit-seeking cyberattacker's expected benefit – as shall be examined in the case studies – often amounts to multiple millions of U.S. dollars. Thus, the package of informal sanctions tends to neither directly deny nor indirectly outweigh a profit-seeking cyberattacker's expected benefits.

On the following page, Table I summarizes the predicted effects of informal sanctions upon each of the three motives.

TABLE I. DETERRENT EFFECTS BY CYBERATTACKER MOTIVE

Motive	***Effect of informal sanctions***	***Effect on deterrence inequality***	***Deterrent result***
Status-seeking	Attack to face denies objective of status, lowering expected benefit *(B)*.	It becomes more likely that $(P_C)(C)$ exceeds a lowered $(P_B)(B)$.	Specific deterrence, and hence general deterrence, is likely achieved upon publicization of the bare indictment.
Profit-seeking	Informal sanctions tend to neither directly deny nor indirectly outweigh the objective of monetary profit.	Since informal sanctions probably do not raise $(P_C)(C)$ enough to outweigh the high $(P_B)(B)$ for profit-seeking motives, $(P_C)(C)$ is not likely to exceed the high $(P_B)(B)$.	It is unlikely that bare indictments will achieve any specific deterrent effect. Therefore, it is also unlikely that bare indictments will achieve general deterrence.[8]
Thrill-seeking	Practical consequences can indirectly outweigh the objective of emotional thrill, as they can raise expected cost *(C)* and can raise expected probability of cost (P_C).	Especially considering that $(P_B)(B)$ is already low for thrill-seeking motivations, a raised $(P_C)(C)$ likely exceeds a low $(P_B)(B)$.	Specific deterrence is likely achieved when the indictment is made known to the indicted actor. General deterrence is likely achieved upon publicization of the bare indictment.

[8] General deterrence is unlikely unless some other mechanism of bare indictments applies, such as if the nation-state of the indicted individual reacts to bare indictments' attacks to face and such reaction has a deterrent effect. In Section 3.3, I discuss why these attacks to face can be imputed as attacks to national status.

3.2.0. How to Determine Motive; Examples

Since criminological methods may be unfamiliar to some readers, Section 3.2.1. gives a brief overview of two methods by which motive is determined in criminological studies and criminal investigations. In Section 3.2.2., I conduct the qualitative behavioral analysis method to analyze cyberattack examples, highlighting the factors that lead to the categorization of motive in each example. Then, in Section 3.2.3., I address some potential objections regarding other cyberattacking motives that might be included in the framework. Section 3.2.4. summarizes the behavioral indicators of cyberattacker motive. At the end of that section, I provide a table summarizing the behavioral indicators for each categorization of motive.

3.2.1. The Concept of Motive; Two Methods of Determining Motive

An important thing to know about the concept of motive is that motive is usually not a formal consideration in making determinations of wrongdoing under criminal law (Hessick 2006, 89-90). While motive is usually not a formal consideration in criminal law, determining motive can be a crucial step in conducting a criminal investigation (Petherick and Turvey 2008, 273-274). For example, determining motive can help identify who was the perpetrator of a crime, since persons who do not hold that motive are unlikely to have been the perpetrator (Petherick and Turvey 2008, 274). The separability of motive and indictment can be an advantage for study sampling, since it is unlikely that the sample will have a bias wherein only actors who have a certain motive are indicted.

Motive, which can be broadly defined as an offender's reasons for committing a crime (Petherick and Turvey 2008, 274-275; Chiu 2005, 664), is an internal inclination (Leonard 2001, 447). Given that motives exist in the mind of an offender and – as with internal feelings of shame and guilt – are not externally perceivable in themselves (Petherick and Turvey 2008, 275), there are two prevailing criminological methods to determine an offender's motive. One method is to conduct an interview with the offender (Scully and Marolla 1984, 531; Neufeld 2010, 9). Although this method has the advantage that the information gathered will be obtained directly from the offender, it is logistically more burdensome because it relies on arranging for the offender and the interviewer to converse with each other. Moreover, the information gathered may be more prone to being unreliable; the offender may be unclear about the offender's own reasons, or the offender might attempt to deliberately mislead the interviewer as to the offender's motive (Petherick and Turvey 2008, 275).

A second way to determine motive is by looking to the "behavioral evidence" revealed by the circumstances of the crime's perpetration and the identity of the crime's target (Petherick and Turvey 2008, 275; Neufeld 2010, 6-9; Mosechkin 2021, 4-7). Considering the wide range of human behavior, it would be a difficult task to arrive at any comprehensive list that covers *in detail* all possible behavioral indicia of a given motive; although criminologists who employ the behavioral analysis method may construct general frameworks and give examples, it is usually infeasible for the examples to be exhaustive of all detailed circumstances that could arise. Therefore, this method of determining motive is heavily dependent on qualitative analysis that asks what motives would be consistent with observed behavioral evidence (Petherick and Turvey 2008, 275; Neufeld 2010, 7;

Mosechkin 2021, 7-8). In short, the qualitative behavioral analysis method of determining motive centers on the question of what motives would be furthered by the observed behavior.

This second method, behavioral analysis of motive, is utilized by this project. The general framework employed here is the typology of three common motives of cyberattackers: status-seeking, thrill-seeking, and profit-seeking. Recall that there are two types of status-seeking – prestige-seeking and dominance-seeking – which brings the total number of motives to four. Since there are innumerable possibilities for cyberattacker behavior in any given cyberattack, giving an example for each of the four motives used by this project's framework may not only help conceptualize each motive, but may also be illustrative of how to conduct the second method.

3.2.2. Conducting Behavioral Analysis of Motive on Four Examples

The following four situations each concern cyberattacks. For each of the four, I analyze the circumstances of the cyberattack to yield a result as to which of the four motives was likely at play. To prevent definitional circularity between the examples and the case studies, none of the following examples coincide with case studies in which an indictment was issued.

The August 2021 data breach of wireless carrier T-Mobile is arguably an example of a cyberattack primarily motivated by thrill-seeking. In August 2021, a cyberattacker obtained unauthorized access to the servers of T-Mobile and took the personal data of over forty million T-Mobile customers (T-Mobile 2021). T-Mobile disclosed that this personal

data included customers' names, dates of birth, Social Security numbers, phone numbers, and driver's license numbers (T-Mobile 2021). Soon, this valuable data taken from T-Mobile was purportedly offered for sale online to any member of the public (Vaas, August 16, 2021). Although it could be argued that this cyberattack was primarily profit-seeking due to the valuable nature of the taken data and the offer of sale, the extremely low price for the data – less than one penny per data record (Vaas, August 16, 2021) – when each data record's capability to be used in identity theft schemes could have commanded a much higher price contradicts the contention that the cyberattack was primarily motivated by profit-seeking. It seems as though the sale of the data were an afterthought, not a goal of the cyberattack. Given what cybersecurity practitioners recognized as the poor state of T-Mobile's cybersecurity defenses, it is more likely that the perpetrator of this cyberattack was motivated by emotional thrill, mounting the cyberattack 'just for fun' or 'just because.' Indeed, a 21-year-old U.S. national physically located in Turkey came forward to claim credit for the cyberattack, explaining the technical details of the cyberattack's execution and providing screenshots of T-Mobile's internal computer systems so as to verify his identity as the perpetrator (Vaas, August 2021b). His proclamation that T-Mobile's cybersecurity was "awful" (Walsh 2021) confirmed cybersecurity practitioners' assessments of T-Mobile's cyber defenses (Vaas 2021b). The U.S. national's proclamation could be interpreted as evidence of status-seeking – attempting to assert his superior status over T-Mobile's in the social hierarchy – but the evidence does not indicate that the U.S. national attempted to raise his status by developing a prestigious reputation as a skilled cyberattacker. Being skilled enough to take advantage of cybersecurity one characterizes as "awful" is not a very high level of skill, so despite this situation having the

potential to increase the perpetrator's prestige, the apparent perpetrator of the T-Mobile data breach did not demonstrably take advantage of the prestige-increasing potential of this situation. Given the behavioral evidence yielded from looking to the circumstances of the cyberattack's perpetration, the T-Mobile data breach was arguably primarily motivated by thrill-seeking.

That motive can be contrasted with the clearly dominance-seeking motive of the April 2007 cyberattacks against Estonia. The widespread DDoS cyberattacks (Stiennon 2015, 7) rendered inaccessible the computer systems of "Estonian banks, media outlets and government bodies" (McGuinness 2017). These DDoS cyberattacks, which crippled both civilian and governmental computer operations, were technically attributed to Russia-based cyberattackers apparently supported by the Russian state (Stiennon 2015, 17). Given that these DDoS cyberattacks closely followed pro-Russia political protests against Estonia (McGuinness 2017), the circumstances of the cyberattacks' perpetration and the identity of the target supports an argument that the April 2007 cyberattacks against Estonia were primarily motivated by dominance-seeking. It seems that the Russian nationals to whom the cyberattacks were technically attributed sought to publicly raise their state's status by publicly suppressing Estonia's status. The cyberattacks were a demonstration of social superiority, not a profit-seeking attempt to garner economic advantage; despite causing chaos by crippling Estonian computer systems, there was no significant taking of data that could then be monetized. Although the perpetrators might have derived some emotional thrill from perpetrating these cyberattacks, the context of the political protests suggests that the perpetrators were primarily motivated by dominance-seeking rather than thrill-seeking. Indeed, resonating with how some international

relations scholars have focused on status as an impetus for initiation of interstate conflict, Richard Stiennon writes that the DDoS cyberattacks against Estonia are widely regarded by scholars as the first real-world example of "cyber warfare" (Stiennon 2015, 16). Therefore, looking to the Estonian identity of the target and the circumstances of the cyberattacks' perpetration – the anti-Estonia political context and the DDoS rather than data theft – gives behavioral evidence that these cyberattacks were primarily motivated by dominance-seeking.

Dominance-seeking is one path by which to conduct status-seeking; the other path of status-seeking is prestige-seeking. The prestige-seeking motive can be seen in the 2009 "Operation Aurora" series of cyberattacks against around thirty U.S. private firms such as Google, Adobe, Yahoo, and Northrop Grumman (Shakarian et al. 2013, 145). In their case study of Operation Aurora, Paulo Shakarian, Jana Shakarian, and Andrew Ruef write that the cyberattacks can be technically attributed to Chinese nation-state actors who were likely acting at the Chinese government's command (Shakarian et al. 2013, 148-150). The apparently Chinese state-sponsored cyberattackers attempted to take the firms' intellectual property pertaining to proprietary technology (Shakarian et al. 2013, 145-146). A cyberattack that attempts to take data relating to markers of prestige can be categorized as motivated by prestige-seeking. As will be discussed in Chapter 4 of this project, the Chinese state conceives of business development and scientific advancement as markers of prestige. By extension, then, cyberattackers who are acting on behalf of the Chinese state are carrying out cyberattacks motivated by prestige-seeking. Since the apparently Chinese state-sponsored cyberattackers who executed Operation Aurora were taking what the Chinese state conceives of as markers of prestige, Operation Aurora can be categorized as

cyberattacks primarily motivated by prestige-seeking. This categorization is notwithstanding that the taken intellectual property likely has significant monetary value. There does not seem to be any indication that the taken intellectual property was monetized; for instance, there is no evidence that the Operation Aurora cyberattackers offered the intellectual property for sale back to the Chinese government or placed it on the open market. These factors make it unlikely that Operation Aurora was primarily motivated by profit-seeking. Even though the taken data may have been financially valuable, the data itself also held significant prestige value in this context, and the monetary value of the data was not leveraged. Hence, Operation Aurora's data theft cyberattacks are best categorized as primarily motivated by prestige-seeking.

By contrast, an example of data theft cyberattacks primarily motivated by profit-seeking is the 2015 data breaches of the U.S. Office of Personnel Management ("OPM"), an American governmental agency that handles human resources matters concerning employees of the U.S. federal government. OPM originally estimated that the number of U.S. federal employees whose data was compromised by the cyberattacks was 4.2 million, but the number was later estimated to be 18 million (Perez and Prokupecz 2015) and was finally updated to over 22 million (Nakashima, July 09, 2015). The U.S. technically attributed these cyberattacks to Chinese state-sponsored actors (Nakashima, July 09, 2015). Upon first glance, the profit-seeking motive of this cyberattack may seem counterintuitive; if the perpetrator was thought to be a state, and the target was also a state, then why would the motive not be primarily status-seeking? Even though these cyberattacks did not take currency, the highly valuable nature of the targeted data supports a contention that the cyberattacks were primarily profit-seeking. A major component of

the data taken through unauthorized access to OPM's computer systems was detailed personal information pertaining to the background investigations of U.S. federal security clearance holders: according to U.S. government officials quoted by *CNN*, "hackers accessed a database storing government forms used for security clearances, known as SF86 questionnaires, which contain the private information of multiple family members and associates for each government official affected" (Perez and Prokupecz 2015). Access to this sensitive data could have enormously profitable implications for a state actor. For instance, this data would enable a state actor to reveal the identities of U.S. intelligence operatives. Moreover, even where a U.S. federal employee was not covert and the U.S. federal employee's identity may have already been known to the foreign state actor, access to the detailed personal information disclosed in security clearance background investigations can sustain blackmail schemes or support other espionage-related forms of exerting psychological pressure to influence the actions of a U.S. federal employee, such as by approaching federal employees' minor children or their other vulnerable family members, friends, and associates (Adams 2016). While this example illustrates why the taking of a wide-ranging cache of data can be immensely 'profitable' to a nation-state actor and therefore be categorized as profit-seeking behavior even when there is no indication that the taken data is further monetized, it is important to note that *any* taking of a wide-ranging cache of personal data is likely motivated by profit-seeking. This is because personal data such as that taken in the OPM data breach can be used to support identity theft schemes, in which the identity thief uses the personal data to pose as the victim; the identity thief can then use the victim's credit cards to make purchases, empty out the victim's bank accounts and take the victim's savings, or commit other actions that directly

garner monetary profit. The highly valuable – one might even say "invaluable" – nature of the data that was targeted by the 2015 cyberattacks against OPM supports an argument that the cyberattacks were primarily motivated by profit-seeking.

3.2.3. Objections to Categorizations in the Motive Framework

With those examples of cyberattacks having been analyzed, there are four related objections that could be levelled against the categorizations in this project's motive framework.

First, it could be argued that all cyberattackers – especially nation-state cyberattackers – derive some prestige or dominance value from the action of being able to gain unauthorized access to the computer systems of a rival; even before the cyberattacker has taken any data, the cyberattacker would be demonstrating superior skill and capability. I would rebut this objection on both conceptual and analytical grounds. Conceptually, the objection is incompatible with the public and social nature of garnering status. Holding a high rank in a social hierarchy is dependent on recognition of other members in that hierarchy; therefore, the status-gaining effect of an action that might garner prestige is optimized by making the action common knowledge. Accomplishing mere unauthorized access without public knowledge does not increase prestige. Moreover, if the unauthorized access is unknown even to the target, then unauthorized access cannot display dominance. In effect, nation-states infrequently publicize their cyberattacking activity by making it common knowledge, so it is unlikely that unauthorized access is uniformly a status-seeking action. In prestige-seeking cyberattacks, the holding of the prestige asset can subsequently

be made public, whereas the cyberattack that took the prestige asset is not usually publicized by the purported perpetrator of a prestige-seeking cyberattack. Analytically, collapsing almost all cyberattacks into the category of status-seeking would yield little insight into the deterrence mechanism. Even if all cyberattacks are, in truth, motivated by 'status-seeking' in some form, categorizing them all as status-seeking means that there is no variable input to yield different outcomes as to whether deterrence was accomplished.

Second, it could be argued that 'causing damage to computer systems' should be categorized as a distinct motive. My answer to address this objection is that causing damage is an outcome, not a motivation. As causing damage is part of the definition of a cyberattack, it would be logically circular for damage-causing to be a motive for the cyberattack. This would be like saying that the reason for committing a crime was 'to commit the crime'; there is little analytical value to be gleaned from this circular statement. Just as international relations scholars have shown that nation-states wage wars in order to make status gains, and just as criminology takes account of varied reasons for committing the same sorts of crimes, I would argue that there must be some underlying reason – a motive – to cause damage. Damage-causing that seems to be perpetrated for no reason other than 'for the sake of causing damage' is not really perpetrated for no reason; it would be categorized as thrill-seeking for emotional benefit, since such a cyberattack would otherwise be an inexplicable waste of a cyberattacker's expected costs such as resources, time, effort, and attention. Likewise, causing damage for a strategic objective – such as causing damage to distract the enemy's attention or to drain the enemy's resources – might be categorizable as profit-seeking, since the cyberattacker seeks to gain an economically valuable benefit that does not relate to status or thrill. Again, I would argue that there is no

analytical clarity added from considering 'damage-seeking' a distinct motive. Since cyberattackers have various reasons for the outcome of causing damage, 'damage-seeking' is not predictive of whether a cyberattack will be deterred by bare indictment.

Third, it could be objected that 'increasing strategic defense capability' should be added as a distinct motive among nation-states. This objection resonates with Shakarian et al.'s conceptualization of China's military-strategy-influenced motive for taking intellectual property (2013, 116-120). I would respond that nation-state cyberattackers have less costly and less risky ways to increase strategic defense capability than by conducting cyberattacks. If the nation-state sees the cyberattack itself as useful practice for its cyberattackers to develop skills, then the deterrence equation would predict that the nation-state should hold internal cyberattacking war games rather than conduct actual cyberattacks that put the cyberattackers at risk of legal liability and put the nation-state at risk of international condemnation. If the nation-state seeks to use the cyberattack to take from inimical nation-states intelligence data that could reveal the state of the enemies' defenses or bolster the nation-state's own capability, then the reason for so doing is probably traceable to profit-seeking or status-seeking. 'Obtaining invaluable data,' including intelligence data, can be categorized as profit-seeking due to the highly valuable nature of data; similarly, given that many wars are fought over status and that defensive capability may itself be a prestige asset, a cyberattack that takes intelligence data might be categorized as status-seeking based on contextual circumstances. Moreover, as with the other two objections, a 'strategic-advantage-seeking' category is not predictive of the deterrent outcome. Bare indictments do not directly deny strategic advantage and are unlikely to indirectly outweigh strategic advantage, yet bare indictments have arguably

deterred some cyberattacks that take strategically useful technological data, as is shown by the Su Bin case study in which specifications for American military aircraft were taken by an apparently Chinese state-sponsored actor who was eventually convicted (*Su Bin* plea agreement, 28). For a full rebuttal to the related counterargument that a "national security purpose" increasingly underlies Chinese nation-state cyberattacks, see Chapter 4.

Fourth, it could be argued that "spreading disinformation" should be categorized as a distinct motive. This objection appears compelling given the seeming rise of cyberattacks used to obtain unauthorized access to networks that can then be used to mount disinformation campaigns: the deliberate spreading of false information to sow confusion and destabilize the target. However, just as I have argued that various motives can underlie the 'criminal' aim of causing damage, I would point out that various motives can underlie the mounting of a disinformation campaign, which is better conceptualized as a harmful action in itself than a reason for the harm-causing action. Thus, a cyberattack that is instrumental in a disinformation campaign is usually best analytically categorized as demonstrating a combination of mixed profit-seeking and dominance-seeking. See Chapter 5 for further analysis of motive in cyberattacks used to carry out disinformation campaigns.

3.2.4. Behavioral Indicators of Cyberattacker Motive

To summarize the categorizations utilized when conducting a behavioral analysis of cyberattacker motive, a cyberattack was likely primarily motivated by **thrill-seeking** when the cyberattack seems to have been executed for no apparent reason. Another way of phrasing this is that thrill-seeking might initially appear like the absence of motive; any

indicia of profit-seeking or status-seeking seem weak. Despite mainly hinging on the absence of a condition, a finding of thrill-seeking becomes more convincing if there is a positive indicator: when the purported cyberattacker issues taunts against the victims or investigators, this suggests thrill-seeking motives because the taunts likely indicate that the cyberattacker wishes to enhance the feeling of emotional thrill. This is the weakest type of cyberattacker motive, as 'having fun through wreaking havoc' might be conceptualized as not very compelling of a motive. Since their expected benefit *B* is quantitatively very low, these cyberattackers will be more inclined than others to select vulnerable or opportune "easy targets," based on low expected weighted cost or high expected probability of benefit. Because thrill-seeking cyberattackers tend to be weakly motivated, I suggest that a behavioral analysis of cyberattacker motive start with thrill-seeking as a baseline assumption and look for whether any taunts were issued.

A cyberattack whose sole objective is to disable or destroy the target's computer systems is likely a **dominance-seeking** cyberattack. This means that all DDoS cyberattacks are presumably dominance-seeking. The exception is if the disablement or destruction seems instrumental in achieving some other objective, such as distracting the enemy or diverting its resources in preparation for executing a kinetic attack. However, just as status-seeking is often a reason for the initiation of interstate wars, dominance-seeking is frequently an underlying motivation for cyber warfare; thus, if a cyberattack would arguably be characterizable as an "act of cyber warfare" – whose definition is further discussed in Chapter 8 – then this may indicate that the cyberattack is dominance-seeking.

Profit-seeking is another motive to mount cyberattacks. A taking of digital currency, being monetarily fungible, is usually an obvious indicator of profit-seeking. Taking into account the valuable nature of data, any taking of a wide-ranging cache of data such as personal details may also be characterized as profit-seeking. This is not only because personal information can sustain lucrative schemes of blackmail or identity theft, but also because even seemingly innocuous data can be invaluable intelligence. As raw data is a valuable commodity, the taken data in a profit-seeking cyberattack usually would have a very high resale value. Taken data does not necessarily need to be monetized for a cyberattack to have been motivated by profit-seeking, but selling any taken data or any software used in the cyberattack is a convincing factor that suggests the cyberattack was conducted with an eye toward economic profits.

While a baseline assumption can be that a taking of data is profit-seeking, this assumption does not hold if the data that is taken directly corresponds to an arguable marker of prestige; a cyberattack through which markers of prestige are taken is **prestige-seeking**. If the circumstances indicate that the taken data coincides with markers of prestige, the cyberattack is primarily motivated by prestige-seeking notwithstanding that the taken data may carry a very high resale value.

This characterization of prestige-seeking clarifies once more why bare indictments achieve an attack to face. Cyberattacks involving unauthorized access can be instrumental to data theft in which markers of prestige are taken; in a bid to gain status, the cyberattacker can then publicize the cyberattacker's ownership of these markers of prestige. My theory does not conceptualize unauthorized access itself as a prestige-seeking

action. Recall that information relevant to prestige cannot affect status unless the information is known to others, as mere possession of markers of prestige does nothing to increase social rank if possession is kept unknown to the other members of the social hierarchy. It is the taken data relating to markers of prestige that the prestige-seeking cyberattacker will publicly present in a bid to gain status. Hence, in this theory, a prestige-seeking cyberattacker would not care whether it is known to the other members of the society that the cyberattacker was the perpetrator of a given cyberattack. However, that prestige-seeking cyberattacker would care if the publicization of a bare indictment subsequently presents the cyberattack as a criminal act, since this attack to status would directly undermine the objective of gaining status.

By contrast, in a dominance-seeking cyberattack, the destructive cyberattack itself may be the dominance-seeking action. A given actor cannot gain prestige from holding markers of prestige unless it is known to the other members that the actor holds those markers of prestige; likewise, a given actor cannot gain prestige from demonstrating arguably admirable qualities – such as the ability to mount a cyberattack – unless it is known to the other members that *this actor* was the one who demonstrated those admirable qualities. However, establishing dominance is not necessarily dependent on the other members knowing who executed the dominant action. This is because, conceptually, whether another member's social rank was suppressed occurs irrespective of whether the other members recognize who was doing the suppression. Therefore, a cyberattack that disables or destroys a target's computer systems can be itself dominance-seeking. Another indicator of dominance-seeking is when the cyberattack communicates messages that undermine the target. The difference between a taunting message and an undermining

message is that taunting messages usually express insincere regret or boast that the investigator or victim will be unable to catch the cyberattacker; by contrast, an undermining message may be an insult, menacing exclamation, or falsehood.

In summary, any cyberattack can be thrill-seeking, since thrill-seeking cyberattacks seem to be committed 'for no apparent reason.' A convincing indicator of thrill-seeking is taunting the victims or investigators. To analyze a cyberattack involving unauthorized access that leads to data theft, one must look to the nature of the taken data. Data theft can be assumed to be profit-seeking if the data carries inherent monetary value, such as if credit card numbers or digital funds were taken. Because of the valuable nature of raw data, the taking of any type of data – including personal details or intelligence information – may be profit-seeking; strategic operational value can be conceptualized as a type of profit. However, if the taken data directly represents what the alleged cyberattacker arguably sees as markers of prestige, then the cyberattack involving unauthorized access that leads to data theft is categorized as prestige-seeking. Finally, a dominance-seeking cyberattack is one whose most salient feature is destroying or disabling a target's computer systems; dominance-seeking is also exhibited in a cyberattack that communicates messages undermining the target.

Table II, which appears on the following page, summarizes the factors that indicate each motive and gives some examples of cyberattacks primarily motivated by the corresponding motive.

TABLE II. INDICATORS AND EXAMPLES OF PRIMARY MOTIVE FOR A CYBERATTACK

Motive	*Indicators*	*Selected examples*
Profit-seeking	- Cyberattack is used to take wide-ranging cache of data (such as personal details), AND/OR - Cyberattack is used to take financial data (such as credit card numbers), AND/OR - Cyberattack involves taking of digital funds or digital currency - Purported cyberattacker takes steps to further monetize any taken data (such as offering taken data for sale on open market) - Purported cyberattacker further monetizes any software used to execute the cyberattack (i.e. offers the software for sale)	2015 data breach of U.S. Office of Personnel Management records Lazarus case study [NK-01] Anthem case study [XNA-06] Equifax case study [XNA-07]
Status-seeking	Status-seeking via **Prestige-seeking**: - Cyberattack is used to take data directly relating to an arguable "marker of prestige" - Monetary value of taken data is *not* leveraged, or any leverage is suboptimal or indirect (if cyberattacker accepts compensation for executing cyberattack, compensation is not primarily tied to taken data's monetary value)	2009 "Operation Aurora" cyberattacks PLA Unit 61398 case study [XNA-01] Su Bin case study [XNA-02] Mabna Institute case study [IRAN-05]
	Status-seeking via **Dominance-seeking**: - Cyberattack disables and/or destroys target's computer infrastructure - Cyberattack is used to communicate messages that undermine (not just taunt) the target - Cyberattack could also be characterizable as an act of "cyber warfare"	2007 DDoS attacks against websites of Estonia's government, media, and financial entities U.S. Financial Industry DDoS attacks case study [IRAN-02] 2022 cyberattacks against Ukraine's banking websites and government computers
Thrill-seeking	- Purported cyberattacker taunts the victims and/or investigators of the cyberattack - Purported cyberattacker does *not* monetize any taken data or any software used in the cyberattack (or monetization is extremely suboptimal) - Purported cyberattacker seems to select 'easy targets,' based on opportunity and/or target's apparent vulnerability	2021 T-Mobile data breach SamSam Ransomware case study [IRAN-06]

3.3.0. Theorizing Public Criminalization as Imputed Responsibility and as an Attack to Face

This section provides a theoretical foundation for **H4** and **H5** by discussing why the public criminalization achieved by the issuance and publicization of a bare indictment against a foreign national can reflect poorly on the foreign national's nation-state and therefore provoke a response from the nation-state. To establish why nation-states would respond at all, I first discuss how Healey's spectrum of nation-state responsibility resonates with the *respondeat superior* principle. I analogize the position of the nation-state to the role of the superior in attribution theory's principle of imputation of responsibility from a superior to a subordinate. Then, I examine why the stakes are especially high for a nation-state against whom the informal sanction of attack to face is imputable. Because a nation-state that cares about national status will have invested a high amount of resources into status-seeking, that nation-state has more to lose if the objective of national status is denied.

Here again are **H4** and **H5**:

- **H4**: The deterrent effect of a bare indictment issued against an alleged cyberattacker will tend to be applicable against that alleged cyberattacker's foreign nation-state in accordance with the principle of *respondeat superior*.
- **H5**: Given that many nation-states care about national status, nation-states against whom bare indictments are imputable will be sensitive to the applicable deterrent effects of the "criminal naming-and-shaming" attack on face that bare indictments achieve.

Their corresponding predictions, **P4** and **P5**, are as follows:

- **P4**: Even though the nation-state itself is not a named defendant, the nation-state government may issue an indignant public statement in response to a bare indictment of individuals alleged to be cyberattacking on the nation-state's behalf.
- **P5**: When a publicized bare indictment is applicable against a nation-state that cares about national status, the nation-state will likely react by attempting to recover status.

3.2.1. Respondeat Superior and the Nation-State

Assume that a given actor has been accused of wrongdoing. When it becomes known that the actor carried out this misconduct under a supervisor's oversight, then it is likely that assignments of blame will fall on the supervisor. As Hamilton theorizes, "Authorities may be *held responsible, legally or morally* [emphasis added], as a function of expectations attached to their role rather than causality per se: What they should have done, seen to, or prevented, rather than anything they actually did" (1986, 120). Thus, a subordinate's misconduct can reflect poorly on a superior. Essentially, the condition necessary for responsibility to be imputed from a subordinate to a superior is the control the superior is perceived to hold over the subordinate's misconduct.

Conceptually, imputed responsibility is not all-or-nothing, but rather, is gradated and is additive. Hamilton's experiment conceives of responsibility as representable by percentages; for a given instance of subordinate misconduct, the superior may be assigned

a higher, lower, or equal proportion of responsibility vis-à-vis the subordinate. If the superior's control is the necessary condition for responsibility over a subordinate's misconduct to be imputed at all, then the proportion of imputed responsibility might directly relate to the superior's level of control.

This gradated conceptualization of responsibility resonates with Healey's (2011) framework of a *spectrum* of nation-state responsibility for cyberattacks perpetrated by its nationals. Healey presents ten categories on his spectrum, and he divides the ten categories in three groups in accordance with the level of nation-state participation in the cyberattack (2011, 59-61). Each group might be rephrased as 'the nation-state government has *insufficient capability* to stop the cyberattacks perpetrated by its nationals,' 'the nation-state government *condones*, supports, or benefits from cyberattacks perpetrated by its nationals,' and 'the nation-state government *actively orders* or participates in cyberattacks.' Correspondingly, Healey theorizes that nation-states can be seen as increasingly responsible for these cyberattacks as the level of nation-state involvement in the cyberattack increases. For instance, if the nation-state government was itself participating in the cyberattack, then presumably it would have a high level of control over whether the cyberattack was perpetrated; not only is the nation-state highly likely to have responsibility for the cyberattack imputed to it, but the proportion of imputed responsibility would likely be high.

Healey's theory suggests that even though a nation-state is an entity rather than an individual, responsibility for cyberattacks can be attributed to this entity because of – and in accordance with – the level of control the nation-state is perceived to hold over its nationals' cyberattacks. Thus, the nation-state is like the superior in the *respondeat*

superior hierarchical relationship, while the foreign national is like the subordinate. This analogy is the basis for theorizing that the *respondeat superior* principle applies to imputed nation-state responsibility for cyberattacks.

Although I invoke "*respondeat superior*" as shorthand for "attribution theory's principle of responsibility imputation from a subordinate to a superior," this is not to argue that the legal principle of *respondeat superior* necessarily applies to make a foreign nation-state literally criminally liable for the alleged law-violating cyberattacks of its nationals. What matters for the purposes of this project is not the legal liability, but rather, the socially constructed moral assignment of responsibility and blame. Because of *respondeat superior*'s alignment with attribution theory's principle of responsibility imputation, *respondeat superior* can be a helpful way to conceptualize the assignment of blame that attribution theory predicts would be mentally contemplated by any person to whom the relevant pieces of information are communicated.

3.2.2. Analogizing the Nation-State to the Superior; Why The Stakes Are Higher

When a bare indictment has been issued against a foreign national, the role of that foreign national's nation-state may be analogized to the position of the superior in *respondeat superior*. This is because the condition for *respondeat superior* to apply is likely to be present when a bare indictment is publicized. Hamilton (1986) identified the condition for blame and responsibility for a subordinate's misdeeds to be imputed to a superior: when it is perceived that the superior could have and should have done something to prevent the subordinate's misconduct, then blame and responsibility for that misconduct may be imputed to the superior. States execute actions through individuals

who are agents of the state; in their role as agents, these agents execute actions – which could include cyberattacks – on behalf of the state. Thus, when an agent of the state is labeled a "criminal outcast" and their cyberattacks are labeled "criminal" misconduct, then it is likely that responsibility and blame for the misconduct of cyberattacks will be imputed to the state. The publicization of criminal charges against an agent of the state, particularly when the criminal charges identify the agent of the state as such, makes it common knowledge that the agent of the state has been labeled a "criminal outcast." Correspondingly, a state whose agent has been criminally charged with committing cyberattacks is likely to contemplate that other members of the social hierarchy – with the social hierarchy being the international community – will likely impute the label of "criminal outcast" to that state. This label represents a threat to the nation-state's status.

Extending this logic further, integrating Healey's theory into this analogy suggests that a bare indictment's attack to the nation-state's status may be effectuated not only when there is evidence to indicate that the indicted actor is an agent of the state, but also when the indicted foreign actor is merely a private individual. This is because the *respondeat superior* condition on the perception of nation-state control can still apply, albeit perhaps more weakly, at the lower ends of Healey's spectrum of nation-state responsibility. I theorize that this perception may be additive. Although Healey suggests that a nation-state cannot possibly police every single one of its nationals, I posit that many of these weak attacks to national face – that is to say, many bare indictments against a nation-state's nationals – will still tend to reflect poorly on a nation-state's status. A nation-state that is perceived to allow its private individuals run rampant committing criminal acts would probably see its status in the global order as being under threat. On Healey's

spectrum, the implication would be that the nation-state is deliberately turning a blind eye to *criminal* activity, the worst form of societal misconduct; or that the nation-state is so incompetent that it is incapable of keeping a significant number of its nationals under control, even though as a function of its role *qua* nation-state it should have done so. These implications are inconsistent with both dominance and prestige; thus, a nation-state against whom the label of 'criminal outcast' is even weakly imputable is likely to react to bare indictments if that nation-state is concerned about national status, as are many nation-states.

In contrast to some scholars, I would theorize that the general and specific deterrent effects of a bare indictment are enhanced when the indictment is issued against a state actor rather than a non-state actor. Even further, then, I predict that – especially considering the international relations literature on status-seeking as a prevalent concern for nation-states – any nation-state that cares about its national status in the social hierarchy of the global order may, due to the application of *respondeat superior*, respond to a bare indictment as though it were a threat to national status. Some scholars have predicted that state-sponsored cyberattackers will be more difficult to deter because they are backed by the resources and protection of a nation-state government (Libicki 2009; Bossler 2019). I agree that bare indictments will be unlikely to deter profit-seeking cyberattackers irrespective of the profit-seeking cyberattackers' identity as state or non-state actors, but I theorize that when bare indictments are already likely to deter an indicted actor in accordance with the indicted actor's motive, then nation-states rather than individual actors will be especially sensitive to the informal sanctions imposed by bare indictment.

Some simple hypotheticals can illustrate the contention that the more one has invested in pursuing an endeavor such as status-seeking, the more one has to lose if that endeavor fails. Assume that the two persons in the following hypothetical about prestige-seeking each regard luxury goods as markers of prestige. For illustrative purposes, also assume that all else is held equal, the sole purpose of purchasing the luxury goods is to obtain markers of prestige, and each person does not receive any incidental benefits such as personal enjoyment from the use of the luxury goods. A person who spends $50,000 on luxury goods but fails to garner any gains in status has suffered greater losses than a person who spends only $500 on luxury goods and likewise fails to garner any gains in status. The first person has $50,000 in wasted costs; the second has only $500 in wasted costs. A hypothetical about dominance-seeking might illustrate a similar point. Assume that pestering a victim is a means of establishing dominance. Again, assume that all else is held equal, that the only purpose of the following schemes is dominance-seeking, and each person does not receive any incidental benefits such as emotional thrill from executing the schemes. Arguably, the person who recruits two hundred acquaintances to pester a victim suffers greater losses than the person who recruits two acquaintances to pester a victim, if both of these dominance-seeking schemes fail to garner any gains in status. Even if the effort expended in recruiting is factored out, and even if it is assumed that these dominance-seeking persons will not be providing any monetary compensation to their respective recruits, the difference in scale between these failed operations means that more resources[9] have been wasted in the first dominance-seeking scheme than in the second.

[9] One might conceptualize the type of resource wasted as "human capital."

Given that – as examined in the international affairs literature – states often seek status, it is precisely because states are likely to have invested more resources in status-seeking that bare indictments' denial of status becomes more devastating. This is especially true if the nation-state in question not only cares about status, but is also carrying out status-seeking cyberattacks; this would affirm that the nation-state cares about status, and it would make the loss of resources directly traceable to the indicted cyberattacker. The observation that nation-states back state-sponsored cyberattackers with a higher amount of resources than is typically available to a given private individual should be intuitive, though "more resources" could be quantified monetarily in a variety of ways: by calculating, for instance, how much a nation-state compensates employees, contractors, or other agents who carry out their cyberattacks on behalf of the state. A higher investment of up-front costs – which is to say, drawing upon the resources available to a nation-state – in a status-seeking cyberattack means that the denial of that status-seeking objective results in greater losses. This theoretical proposition also resonates with psychological literature finding that informal sanctions regarding social outcasting have a greater impact on high-ranking persons than low-ranking persons (Karelaia and Keck 2013; Polman et al. 2013; Kakkar et al. 2020). The more one holds, the more one has to lose. The stakes are higher for a nation-state when its status is attacked via bare indictment.

Considering that crimes are theoretically conceptualized as the most severe form of offensive behavior in a society, it follows that the type of misconduct that may reflect most poorly on a superior is *criminal* misconduct. When a bare indictment's attack to face is imputable against a nation-state, the label of 'petty criminal outcast' is not only grossly

incompatible with holding a high rank in the social hierarchy of the global order, but also results in the nation-state's loss of the extensive resources it has invested in status-seeking endeavors such as cyberattacks. For any nation-state that cares about status, the stakes of being subject to an attack on face are high because the nation-state has much to lose. This suggests that nation-states are especially sensitive to the attacks on national face that are achieved by a formal accusation of criminality.

3.4. Theorizing the Shift to Profit-Seeking

This section theorizes **H6**, the hypothesized shift to profit-seeking cyberattacks. I predict a shift away from status-seeking and toward profit-seeking, as well as a similar shift away from thrill-seeking and toward profit-seeking. For simplicity, I will set aside thrill-seeking in the following theoretical illustration, which discusses only status-seeking and profit-seeking in contradistinction with one another.

If bare indictments tend to be an effective specific deterrent against status-seeking cyberattackers but tend not to specifically deter profit-seeking cyberattackers, a hypothesis that follows is that over time, cyberattacks will shift from being motivated by status-seeking to being motivated by profit-seeking; status-seeking will already have been deterred. Likewise, if bare indictments can achieve norm-setting general deterrence against status-seeking cyberattacks, the theory predicts that bare indictments would come to be issued almost exclusively against cyberattacks that are motivated by profit-seeking. Status-seeking cyberattackers would have been convinced that the costs of status-seeking

cyberattacks exceed the benefits. Hence, if the deterrent mechanism of bare indictments is working as theorized, there will be relatively fewer status-seeking cyberattacks to indict.

Assume that, among cyberattackers, some are primarily profit-seeking and some are primarily status-seeking. A third category of cyberattackers is primarily motivated by both profit-seeking and status-seeking. As they are motivated by mixed profit-seeking and status-seeking, this third category is a type of 'mixed-motive' cyberattackers. If the status-seeking cyberattackers are deterred by the expectation that a bare indictment will be issued against them, then they will not commit the cyberattacks. The cyberattackers who are motivated by both profit-seeking and status-seeking may find the expected benefit of profit enough to sway the cost-benefit calculus in favor of perpetrating cyberattacks in which both motives are salient; it is as if the presence of their profit-seeking enables the presence of their prestige-seeking. Some of the cyberattackers who were previously motivated by status-seeking may, with this new information about the expectation of bare indictment, become profit-seeking instead. Finally, since the profit-seeking cyberattackers are unlikely to be deterred by the expectation of bare indictment, they remain likely to commit cyberattacks. As mentioned in the discussion of determining a motive by qualitatively analyzing the circumstances of a crime, motivations become salient in behavior when a cyberattacker commits, or attempts to commit, a cyberattack. The result is that the observable cyberattacks that are committed by the members of this pool of cyberattackers become almost exclusively motivated by profit-seeking.

Legally, indictments against cyberattacks are only issued when a cyberattacker commits, or attempts to commit (see 18 U.S.C. § 1030(b)), a cyberattack. Indictments

under 18 U.S.C. § 1030 – the relevant federal statutory law, as further discussed in Section 3.6. – may not be issued in response to every single cyberattack that is committed or attempted, but they can only be issued in response to cyberattacks that are committed or attempted. If an actor has been successfully deterred from an action, then that actor would not be committing or attempting that action. Therefore, if only the profit-seeking cyberattackers and the mixed-motive profit-seeking status-seeking cyberattackers are committing or attempting cyberattacks, the theory would predict that bare indictments will become issued almost exclusively against cyberattacks wherein profit-seeking is a primary motive. This trend would be proof that bare indictments accomplish norm-setting and achieve a general deterrent effect. It would be logically consistent with CDT's extrapolation that, over time, almost all cyberattackers will contemplate bare indictment as a negative consequence of committing or attempting a cyberattack. Whether this negative consequence will deter them depends on whether they are profit-seeking, status-seeking, or both profit-seeking and status-seeking.

An objection would be that the prediction of bare indictments coming to be issued almost exclusively against profit-seeking cyberattacks is not necessarily indicative of a shift to profit-seeking cyberattacks. Since bare indictments are not issued in response to every cyberattack but rather draw from a pool of cyberattacks, the proportion of profit-seeking versus status-seeking motives salient among 18 U.S.C. § 1030 indictments would not necessarily be representative of the proportion of motives among all the indictable cyberattacks that are committed. In this theoretical situation, a possible alternate route is that, for some intervening reason, it is the investigators and prosecutors involved with issuing a bare indictment who shift to indicting only profit-seeking actors. That is to say,

this alternative explanation of the reason for the trend toward only profit-seeking actors being indicted is that only profit-seeking actors are selected for indictment, and cyberattacks committed by status-seeking actors continue to be committed without being indicted. This remains a possibility, but it is unlikely; as discussed in Chapter 3, motive is generally not a formal consideration in criminal charging of cyberattacks. Where the motive is not a formal component of the crime, investigators and prosecutors usually only consider motive in order to build a coherent legal case. Not only are prosecutors unlikely to pay attention to motive, but also, there does not seem to be a reason why prosecutors would prefer to issue bare indictments against profit-seeking cyberattackers rather than prestige-seeking cyberattackers. As mentioned in Section 3.2., profit-seeking can be assumed whenever an economic benefit to the perpetrator is involved, whereas determining prestige-seeking usually requires deeper analysis that contextualizes the taken data within what the actor considers to be markers of prestige. This means that, without conducting deeper analysis, profit-seeking and prestige-seeking cyberattacks can appear identical to a criminal investigator or a criminal prosecutor; if an investigator or prosecutor would probably not draw a distinction between them, there is no basis upon which for the investigator or prosecutor to exclude prestige-seeking cyberattacks and pursue only profit-seeking cases. Hence, in the absence of a general deterrent effect against status-seeking cyberattacks, there does not appear to be a reason why the persons involved in issuing a bare indictment would deliberately or unconsciously shift to indicting only profit-seeking. Because motive is not a formal consideration in issuing an indictment, for this objection to stand there would need to be some empirical evidence on an intervening reason, such as the deterrent effect of a deterrent measure other than bare indictment

being responsible for the shift, or that new policy dictates that prosecutors and investigators must indeed focus their attention exclusively on profit-seeking cases at the expense of status-seeking cases.

If and when bare indictments achieve a general deterrent effect against status-seeking but not against profit-seeking, then over time bare indictments will come to be issued only against cyberattackers primarily motivated by profit-seeking and against cyberattackers primarily motivated by both profit-seeking and status-seeking. Another way of phrasing this is that profit-seeking will come to be a salient motive among almost all indicted cyberattacks. In keeping with the prediction that primarily status-seeking cyberattacks and primarily thrill-seeking cyberattacks will no longer be present among bare indictments but profit-seeking attacks will, this means that mixed-motive cyberattacks that have profit-seeking as one of the primary motives will still be committed; I predict that over time mixed-motive thrill-seeking and profit-seeking cyberattacks would still be present among bare indictments, and mixed-motive status-seeking and profit-seeking cyberattacks would still be present among bare indictments, but mixed-motive thrill-seeking and status-seeking would not. This also means that mixed-motive cyberattacks in which all three motives are salient will, likewise, still be present among bare indictments because one of those motives is profit-seeking, against which bare indictments are unlikely to achieve deterrent effects. As theorized above, it is as though the profit-seeking motive enables the presence of the motives that would be otherwise deterred, since the presence of profit-seeking motives can still tip the cost-benefit calculus such that the expected benefits of monetary profit exceed the expected weighted costs from bare indictments' denial of the status-seeking objective.

Because profit-seeking is usually undeterred by bare indictment, any cyberattacks that have profit-seeking as a primary motive will continue to be committed or attempted; since only cyberattacks that are committed or attempted make it into the pool of indictable cyberattacks, over time only cyberattacks motivated by profit-seeking will be subject to bare indictment. This would be proof that the bare indictment's deterrent mechanism is working as hypothesized, by deterring status-seeking cyberattacks and thrill-seeking cyberattacks. As successful deterrence means that these criminal acts are never executed, the cyberattacks that never happened are excluded from the pool of indictable behavior.

3.5. Testing the Theory: Methodology and Evidence

To test these hypotheses, I conduct in-depth analyses of case studies in which domestic criminal charges, alleging violations of a law prohibiting cyberattacks, were issued against foreign nationals of a nation that has no extradition treaty with the nation that issued the bare indictment. Within the case studies, I usually first determine the primary motives of the alleged cyberattacker: prestige-seeking, dominance-seeking, profit-seeking, or thrill-seeking. Then, I determine whether and to what extent the bare indictment achieved a deterrent effect. Specific deterrence is evidenced by a sudden halt in recidivist cyberattacks; general deterrence is evidenced by a reduction in similar cyberattacks by other potential offenders. A public response from the indicted actor's nation-state, especially when the text of the response makes direct reference to the bare indictment, confirms that the bare indictment has been contemplated by the nation-state and provides convincing evidence that the nation-state construes the bare indictment as an

attack on national status. In accordance with the before-and-after study design, the most convincing factor to determine that the bare indictment caused the deterrent effect is the timing of the deterrent effect: that indicators of the deterrent effect closely follow the publicization of the bare indictment. Causality can be further supported by addressing and ruling out competing explanations for the deterrent effect. Next, I check whether the combination of motive and deterrent effect is in line with the predictions of the theory. If the combination is in line with the predictions of the theory, then I discuss the elements of the case study that likely contributed to the deterrence success. If the combination is not in line with the predictions of the theory, then I identify and discuss intervening causes that could have contributed to the unexpected result on deterrent effect.

My sources of evidence center on primary texts. To determine the motives of the indicted cyberattackers, I focus on the publicly released information contained in the press release and the criminal charges. It is these publicly released materials that the issuer of criminal charges makes into common knowledge, so the deterrent effect is best understood by looking to the deterrent message that was communicated to the public. For evidence of whether and to what extent a deterrent effect was achieved, I look to publicly released technical attribution reports by private cybersecurity firms or to the publicly released findings of cybersecurity practitioners. Sometimes, further details on the circumstances of the cyberattacks are informative in determining motive. For those further details, I look to secondary sources such as publicly available news reports. News reports on cyberattacks often contain quotes from other cybersecurity researchers, so I also draw upon these news reports to identify and respond to alternate arguments.

In these case studies, I utilize a before-and-after qualitative study design to strengthen the argument that the bare indictment, rather than some other intervening cause, was responsible for achieving the deterrent effect in a deterrence success. As Freedman has written, because a deterrence success results in inaction – the potential offender decides *not* to commit the offense – studies measuring the empirical successes of deterrence theories may encounter an evidentiary issue with determining whether it was a deterrent measure or some intervening cause that led to the inaction: "With deterrence the objective is inaction. Inaction can have many causes, including a lack of interest in action" (2005, 790). To surmount this evidentiary issue, I examine cyberattackers' behavior just before and just after the publicization of a bare indictment against them. If, during that limited timeframe, there is a change in longstanding behavior – such as a sudden stop or a sharp decline in the cyberattacking activity that can be technically attributed to that actor – then it becomes unlikely that some other cause could have intervened in that narrow temporal period. To further rule out competing explanations for the inaction, I assess whether these alternate causes were already present before the bare indictment's issuance; if an alternate cause was already present before the bare indictment was publicized yet this alternate cause failed to achieve a deterrent effect, then it is more likely that the bare indictment rather than the alternate cause led to the deterrence success.

Beyond this basic methodological framework, the structure of each case study varies. For example, some case studies are grouped together and analyzed in tandem to show a larger-scale trend. I also use most of these case studies as a starting point to discuss various remarkable elements of the case, since it is to be anticipated that some features of the theory will be more salient in some case studies than in others. Moreover, I vary the

amount of written analysis devoted to the various aspects of each case study; although all the case studies will connect to the theory on why bare indictments deter cyberattacks, the structure and content of each case study will vary.

In light of the number of case studies this project analyzes, my rationale against equalizing the structures of the case studies is threefold. One, I surmise that reading several structurally similar case studies that conduct equally in-depth analyses of the same basic points *ad nauseam* would be extremely uninteresting for the reader. Two, repetitively focusing on the same elements when the theoretical mechanism has already been demonstrated in another case study would result in missed opportunities to discuss how the theory on bare indictments interacts with the unusual circumstances that may arise in each case, as it is these unusual circumstances that yield useful recommendations for policy practitioners and unique insights on the workings of the theory. Three, the circumstances and outcomes of some cases are better suited than are others' to provide evidence for rebutting counterarguments.

3.6. Case Selection: Why Select on 18 U.S.C. § 1030?

This section justifies the case selection rationale. I select cases involving a U.S. bare indictment alleging that the person or persons against whom it is issued has violated the federal criminal statute 18 U.S.C. § 1030. I select exclusively on what, under U.S. law, is formally known as an "indictment"; I exclude other types of criminal charges.

The reason for studying only U.S. cases is that bare indictment of suspected cyberattackers appears to be an exclusively – or at least mainly – U.S. phenomenon

(Keitner 2019, Hinck and Maurer 2020). Scholars have not identified another jurisdiction that has issued domestic criminal charges – against foreign nationals of a nation that has no extradition treaty with the issuing jurisdiction – accusing those foreign nationals of having violated the issuing jurisdiction's criminal laws by allegedly mounting cyberattacks.[10] It seems that "bare" criminal charges against suspected cyberattackers have not been issued from any jurisdiction other than the U.S.

Why focus on "indictments" rather than other forms of U.S. criminal charges, such as a criminal complaint? Although throughout these case studies I will often advance an argument that other types of domestic criminal charges can achieve a similar deterrent effect against cyberattacks, in the U.S. context "indictments" are the legally appropriate procedural action and are likely to be made common knowledge. Under the Fifth Amendment of the U.S. Constitution, a prosecution for 18 U.S.C. § 1030 must be initiated via indictment by a grand jury, and not via criminal complaint. A criminal complaint alleging a violation of 18 U.S.C. § 1030 can be grounds for an arrest warrant, but once the charged actor is apprehended, an indictment must be issued before that actor can be prosecuted for alleged violations of 18 U.S.C. § 1030. Moreover, in effect, bare indictments for 18 U.S.C. § 1030 are publicly announced by the U.S. Department of Justice ("DOJ") via press release. In contrast, at least one "bare" criminal complaint was not publicly announced by the DOJ; U.S. authorities' apprehension of Chinese national Yu Pingan pursuant to an arrest warrant that

[10] Irrespective of whether the criminal charge is related to cyberattacks, the absence of this phenomenon in national jurisdictions other than the U.S. may at least in part be driven by differences in criminal charging procedure across national jurisdictions. In the U.S., it is entirely routine for formal criminal charges to be issued prior to the apprehension of a charged individual (Federal Bureau of Investigation, n.d.). A contrasting example comes from the United Kingdom, in which formal criminal charges are typically issued *upon* apprehension of an individual (Crown Prosecution Service 2020, 7). In Section 7.6., I discuss how policy practitioners can look to the theory on bare indictments in order to navigate such differences in criminal charging procedure.

was grounded by a criminal complaint (see *Yu Pingan* criminal complaint) was covered by news reports (see Blake 2017), but it does not seem that a DOJ press release was issued regarding Yu's criminal charges. One of the reasons why bare indictments are theorized to achieve an optimal deterrent effect is that they are publicized, usually after unsealing but sometimes only after the "bare" indictment has resulted in an actual apprehension. Every case of 18 U.S.C. § 1030 bare indictment has been publicized via DOJ press release. Even if the criminal charge eventually becomes public knowledge, the suboptimality of non-publicization means that the deterrent effect of a non-publicized criminal charge is predicted to be weakened, so it is not as informative for theory-building. That being said, the Yu Pingan case is the only found case from the four nation-state cyber adversaries studied that was excluded on the criterion of indictment versus other criminal charge. Two other found cases involving criminal complaint – the Su Bin case study and the Lazarus case study – are both discussed in this project because 18 U.S.C. § 1030 indictments were eventually issued against each of these charged actors.

18 U.S.C. § 1030, entitled "Fraud and related activity in connection with computers," is well suited as a case selection criterion because it corresponds to this project's definition of "cyberattacks": unauthorized access to computer systems and / or using cyber means to cause damage to computer systems. Unauthorized access to computer systems can be a crime under 18 U.S.C. § 1030(a)(1) through 18 U.S.C. § 1030(a)(4); using cyber means to cause damage to computer systems can be a crime under 18 U.S.C. § 1030(a)(5). Given that the conduct outlawed by 18 U.S.C. § 1030 coincides with this project's definition of cyberattacks, selecting cases involving charges of 18 U.S.C. § 1030 violations makes it clear

that the cyberattacks themselves, rather than only some type of related conduct such as economic espionage, were identified as the criminal harm to be deterred.

Note that the terminology used in this project is "cyberattack," "cyberattacking," and "cyberattacker," not "hack," "hacking," and "hacker." Many in the cybersecurity world would argue that it is not "hacking" behavior that should be deterred, since "hacking" is too broad of a term; "hacking" can refer, quite neutrally, to using a non-standard means to gain access to a system (Holt 2020; Oliver and Randolph 2020). Moreover, not all hacking behavior is unauthorized, but rather, is legitimated by and valuable to companies who authorize so-called "white hat hackers" or "ethical hackers" to test their systems for vulnerabilities; the companies monetarily compensate these hackers by paying them salaries or by offering rewards called "bug bounties" (Holt 2020; Oliver and Randolph 2020). Because a significant portion of hacking activity is productive rather than illicit, there is a convincing argument that hacking behavior should not be deterred. Indeed, the text of 18 U.S.C. § 1030 does not capture authorized hacking activity as a type of behavior that violates the statute. Thus, it would be less semantically accurate to study 18 U.S.C. § 1030 as a criminalization of "hacking" than as a criminalization of "cyberattacking."

On this note, an objection to using 18 U.S.C. § 1030 as a case selection criterion regards this law's entanglement with controversy, as it has been argued that 18 U.S.C. § 1030 as applied overreaches its legal scope of criminalizing cyberattacks. 18 U.S.C. § 1030 is also known as the Computer Fraud and Abuse Act ("CFAA"); under the name CFAA, the law has been the subject of controversy involving the CFAA's susceptibility to what proponents for CFAA reform have called 'creative prosecutorial interpretations.' These

arguably creative – other apt terms might be "arguably strained" or "arguably contrived" – applications of the law have drawn ire from Internet activists and criticism from legal scholars; central to this criticism is the prosecutorial argument that acting out of compliance with a website's terms of service is tantamount to unauthorized access and therefore can constitute a violation of the CFAA (Electronic Frontier Foundation, n.d.; Zetter 2015).

However, there are two reasons why the disadvantage of controversy should have little bearing on the integrity or reception of this study. First, the subject of the controversy – strained readings of the law – is not directly applicable to the case studies in this project. My research has not yielded any scholarly argument that any of the studied 18 U.S.C. § 1030 indictments issued against foreign nationals were strained interpretations of the law. Neither does my own analysis of the text of any of the indictments I study in this project find basis for arguing that any of the § 1030 charges that this project will discuss in its case studies were contrived readings of the law. Second, two recent policy developments seem to have progressively allayed the controversy. One, in June 2021, the U.S. Supreme Court's decision in *Van Buren v. U.S.* limited prosecutors' ability to make these arguably contrived, broad interpretations of the CFAA. Writing in *Lawfare*, legal scholar Orin Kerr noted that *Van Buren* clarified that the harm criminalized by the CFAA was unauthorized access: "this is a major victory for those of us who favor a narrow reading of the CFAA. It settles that the CFAA is fundamentally a trespass statute. The basic wrong is bypassing a closed gate, going where you're not supposed to go. The CFAA does not make it a crime to break a promise online. It does not make it a crime to violate terms of service" (Kerr 2021). Two, as recently as May 19, 2022, the U.S. DOJ issued and publicly announced its new policy on

CFAA violations; expressly addressing the criticism over the terms-of-service interpretation, the DOJ stated that such actions – while possibly civilly or criminally actionable under laws other than the CFAA – were "not themselves sufficient to warrant federal criminal charges" and therefore are not to be charged under the CFAA (DOJ OPA, "New Policy for Charging Cases," May 19, 2022). Still, to avoid evoking the past controversy associated with this law, throughout the case studies I refer to the law as "18 U.S.C. § 1030" or "§ 1030" rather than the colloquial "CFAA."

In comparison to the history of controversy with the unauthorized access provisions of the CFAA, relatively less attention has been devoted to § 1030(a)(5), which – loosely speaking – regards using cyber means to cause damage to computer systems. This is likely because the scope of this provision is more straightforward. For example, as explored in a 2013 analysis by cybersecurity attorney Shawn E. Tuma, rulings from U.S. federal courts clearly show that mounting a DDoS attack can be a violation of the CFAA (Tuma 2013). Thus, § 1030(a)(5) corresponds to the second half of this project's definition of "cyberattacks."

Given this theory's grounding in CDT, there are significant advantages to selecting cases in which 18 U.S.C. § 1030 is expressly one of the charges. Were the scope of case selection expanded to cases in which 18 U.S.C. § 1030 violations are not alleged, trawling through the text of more indictments and analyzing them for cyberattacking activity might be possible, but in those cases the deterrent message would be muddled. If 18 U.S.C. § 1030 were not expressly charged, it would be unclear to all parties concerned that the cyberattacks themselves – the unauthorized access and / or damage to computers – were

the criminal offenses to be deterred. Beyond conceptual clarity of the deterrent message, selecting on 18 U.S.C. § 1030 is also more efficient. Conducting an automated search for the textual term "18 U.S.C. § 1030" is a more straightforward way to compile data than is qualitatively analyzing the text of criminal charges wherein 18 U.S.C. § 1030 is not named. Indeed, there exist compilations of data regarding charges of 18 U.S.C. § 1030 against foreign nationals from nations that may be described as the U.S.'s cyber adversaries (Hinck and Maurer 2020, Logan and Patel 2020a). Data analysis of one of these data compilations – a dataset entitled "U.S. Sanctions Against Malicious Cyber Actors" (Logan and Patel 2020a) – yields information that forms the structural basis for this case-study-centered project.

3.7.0. Data

This section describes the data used in this project. In Section 3.7.1., I introduce the "U.S. Sanctions Against Malicious Cyber Actors" dataset. I discuss why this project, like the dataset, focuses on § 1030 bare indictments issued against nationals of China, North Korea, Iran, or Russia. These four nation-states – both the state actors and non-state actors thereof – are seen by the U.S. government as 'cyber adversaries,' a category that makes them 'hard cases' for testing the hypotheses on bare indictments. If it can be demonstrated that the bare indictment mechanism can deter even hard cases – strongly motivated nation-state cyber adversaries that have virtually unlimited resources available to protect their government agents and private nationals from prosecution – then the theory should hold true against comparatively easy cases. In Section 3.7.2., I discuss the related reasons

why my project does not focus on nation-state affiliation; nation-state affiliation can enhance the general deterrent effect, but nation-state affiliation is neither necessary nor sufficient for achievement of a deterrent effect. Section 3.7.3. covers data cleaning and supplementation of the dataset; this may serve as an illustration of how quantitative data can be used to support small-*N* qualitative studies. Then, Section 3.7.4. provides an original dataset of § 1030 bare indictments issued against nationals of China, North Korea, Iran, or Russia.

3.7.1. FDD CCTI Dataset on "Malicious Cyber Actors"

The raw data used in finding case studies and structuring this project is a dataset entitled "U.S. Sanctions Against Malicious Cyber Actors." This dataset was compiled by the Center on Cyber and Technology Innovation ("CCTI") at the Foundation for Defense of Democracies ("FDD"). The FDD CCTI dataset was published by Trevor Logan and Pavak Patel online on April 20, 2020. The dataset ostensibly includes only actors whose nationality is Chinese, North Korean, Iranian, or Russian. The dataset holds 192 entries of actors who were subject to either the imposition of U.S. economic sanctions in response to the actor's alleged cyberattacking activity, the imposition of a U.S. indictment in response to the actor's alleged cyberattacking activity, or both. Each of the 192 entries is an actor; the actors could be either individuals or entities. Logan and Patel write that the dataset is not coded so as to determine whether each foreign national is a nation-state actor or a private actor (Logan and Patel 2020a). They suggest that this publicly available dataset can support future studies on bare indictments as a deterrent measure: using this dataset,

"analysts can assess more effectively whether [economic] sanctions and indictments are effective tools to punish or deter malicious cyber activity" (Logan and Patel 2020a).

In accordance with the FDD CCTI's dataset, this project focuses on case studies involving the respective nationals of China, North Korea, Iran, or Russia. I suggest three reasons for narrowing the studied range of indicted cyberattackers to nationals of these four nations. The first reason, data availability, is pragmatic; the FDD CCTI dataset readily includes information pertaining only to nationals of one of these four nations, and it does not include information pertaining to indicted foreign actors from other countries. Some scholars might argue that the range of studied nations should be broadened, because there are other nation-states whose governments engage in cyberattacking activity against U.S. targets and whose state-sponsored actors have been indicted; for instance, Garrett Hinck's and Tim Maurer's 2020 article "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity" studies state-sponsored cyberattackers from five nations, adding Syria as the fifth nation (Hinck and Maurer 2020, 547). Although it may be true that the governments of other countries may mount cyberattacks against U.S. targets, the four nations share a commonality that is not shared by other nations; this commonality forms a logical basis for study organization.

The second reason, then, is that the U.S. government expressly considers the four nations – China, North Korea, Iran, and Russia – to be its cyber "adversaries" (Coats 2018, 5). An official 2018 report entitled "Worldwide Threat Assessment of the U.S. Intelligence Community" issued on behalf of the U.S. Office of the Director of National Intelligence ("ODNI") – a U.S. federal government agency – stated under the section heading "Cyber

Threats" and the subheading "Adversaries and Malign Actors Poised for Aggression," "Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year" (Coats 2018, 5). It is very important to recognize that this report expressly considered not only each nation's respective governmental state-sponsored cyberattackers, but also each nation's respective *private non-state cyberattackers*, to be the cyber adversaries in question; the report specifically discussed "nonstate actors," (Coats 2018, 6) and the section on "Cyber Threats" concluded, "We expect the line between criminal and nation-state activity to become increasingly blurred" (Coats 2018, 6). The ODNI's focus on China, North Korea, Iran, and Russia as the U.S.'s cyber adversaries continues to the present day, as the 2022 version of the ODNI's annual report likewise gives express discussion of the cyber threats emanating from each of these four nations (ODNI 2022, 8; ODNI 2022, 12; ODNI 2022, 15; ODNI 2022, 17); like the 2018 ODNI report, the 2022 ODNI report does not expressly consider any other groups of nationals to be among the U.S.'s cyber adversaries. Thus, the ODNI's categorization of the nationals from these four nations provides a logical and consistent way to focus the range of the study. In turn, then, the third reason to focus the project only upon indicted foreign nationals from nations that the U.S. has categorized as cyber adversaries is that these groups of nationals' categorization as cyber adversaries makes them conceptually 'hard cases' for this project to explain, and therefore well-suited for proving the theory on bare indictments. If it can be shown that bare indictments can deter cyberattackers as formidable as the U.S. government's cyber adversaries, then the theory may be logically predicted to hold against cyberattackers who are more weakly motivated and who are

unable to draw upon the resources of a nation-state that apparently condones, supports, or even directly orders their cyberattacks.

3.7.2. A Focus on Nationality, not National Government Affiliation

Relatedly, two further observations about this project's range of studied data should be noted here. First, it should be noted that none of these four nations is party to a bilateral extradition treaty with the U.S., ergo any § 1030 indictment issued against a national of one of these countries would be a "bare indictment." Second, in accordance with the U.S. government's approach, my presentation of the data makes minimal differentiations between state and nonstate actors. I theorize that bare indictments' deterrent effect turns on the motive, not on the indicted foreign national's identity as a state or non-state actor. Still, the indicted foreign national's arguable level of state affiliation can be relevant for the following two reasons.

One, the indicted foreign national's level of state affiliation determines how strongly the *respondeat superior* principle applies against the nation-state and therefore predicts how likely the nation-state is to respond to the imputed attack on face. In accordance with *respondeat superior*, a nation-state would be likely to respond when an indictment of a government employee or government official is publicized, moderately likely to respond when an indictment of a government contractor – a private individual whom the government directs to mount a cyberattack – is publicized, and not likely to respond when an indictment of a private individual is publicized. The relevant set of hypotheses and predictions – **H4**, **H5**, **P4**, **P5** – concerns to what extent the bare indictment can deter at the

nation-state level, not whether the bare indictment can deter at all. National governmental affiliation may therefore be predicted to enhance the general deterrent effect, but Healey's conceptualization shows that a cyberattacker's national governmental affiliation exists on a continuum. The level of governmental affiliation progressively enhances general deterrence rather than dictates whether deterrence is achieved by bare indictment.

Two, looking to the level of governmental affiliation can aid with analyzing motive using the behavioral analysis of motive method. If the results of criminal investigation show that the indicted individual was acting on behalf of a foreign government, this can provide some helpful context for the motive driving a cyberattack. For instance, if it is alleged or can be shown that the indicted cyberattackers are affiliated with the Iranian government, the inference can then be made that the taking of valuable aerospace defense data – which, as will be discussed, the Iranian state considers to be markers of prestige – was motivated by prestige-seeking rather than profit-seeking. If there is no evidence to indicate that the cyberattackers have any ties to the Iranian government, or if evidence indicates that the cyberattackers put the taken data up for sale on the open market, then the very same taking of valuable aerospace defense data would probably be profit-seeking, not prestige-seeking. This is because a taking of *valuable* data is usually an indication of profit-seeking motives. Using the same hypothetical taking of valuable data as an example, the argument on this cyberattack's profit-seeking motives would be made stronger if the investigation found that the indicted cyberattackers had ties to the North Korean government, since – as will also be discussed – the North Korean state is in need of monetary funds. I theorize that the deterrent effect turns on motive, not on national government affiliation; for the purposes of this theory, an indicted actor's nation-state

affiliation can therefore also be relevant insofar as it helps in conducting the *analysis* of motive.

Thus, as I theorize that an indicted foreign national's affiliation with the national government is neither a necessary nor sufficient condition for deterrence, my project only considers national governmental affiliation where it is relevant to the *respondeat superior* principle or the analytical determination of motive.

3.7.3. Data Cleaning and Data Supplementation

In this section, I provide a brief overview of the data cleaning I performed on the FDD CCTI dataset. This section may be of interest as a template demonstrating how data cleaning can be used as a preliminary step to construct qualitative small-*N* studies, with "small-*N* studies" meaning projects that "seek to investigate chosen cases in depth and in context, rather than making statistical claims based on large numbers" (Gouvea 2017, 1, at footnote 1).

The FDD CCTI dataset includes two types of "sanctions": economic sanctions and criminal indictments. My project centers on criminal indictments rather than economic sanctions. Thus, after exporting the dataset to Microsoft Excel file format, I filtered the dataset by the "Only Indicted" and "Both" categorizations, excluding those entries regarding persons who were "Only Sanctioned." As the export had rendered the "Date Indicted" values in text rather than in dates, I used the DATEVALUE function in Excel to reformat these text cells into dates. To order the indictments chronologically, I sorted the entries by date from oldest to newest.

Not all the indictments involve § 1030, as the U.S. has federal criminal laws pertaining to cyber-related behavior other than what this project defines as "cyberattacks." Therefore, to narrow the range to bare indictments involving "cyberattacks," involving the next step was to determine which indictments involved charges of 18 U.S.C. § 1030. The Tableau worksheet for the FDD CCTI dataset includes charging information in the "Charged Under" category, but the "Charged Under" category was not transmitted in the Excel export.[11] In the Tableau worksheet, 18 U.S.C. § 1030 was usually coded as "Fraud and related activity in connection with computers." Therefore, I created a new column entitled "18 U.S.C. § 1030" in the Excel worksheet, referred to each entry in Tableau, and manually coded each entry as "Y" or "N" based on whether the corresponding entry in the Tableau layout included at least one "Fraud and related activity in connection with computers" charge. For those entries coded "N" in accordance with the absence of a listing in Tableau, I manually verified the negative coding by consulting the text of the corresponding indictment to verify that it did *not* include a charge of 18 U.S.C. § 1030. Where I did find charges under 18 U.S.C. § 1030, I corrected the coding to "Y."

The FDD CCTI dataset on the U.S.'s cyber adversaries included four values that "Nationality" could take. In alphabetical order, these are "China", "DPRK" (meaning North Korea), "Iran," and "Russia." To organize the data by nationality, I created four copies of the Excel worksheet; each copy retained the filters and sorting that had been applied thus far as well as the new "18 U.S.C. § 1030" column. I labeled each copy with a filename corresponding to each of the four "Nationality" values. On each worksheet, I filtered the

[11] Those interested in working with the FDD CCTI dataset may find this suggestion useful: I subsequently discovered that the charging information would be included by accessing the Excel file download link – "Download: Full Dataset (Excel)" – at the bottom of the webpage, as opposed to utilizing the "Download" export function in the lower right corner of the webpage's embedded Tableau worksheet.

"Nationality" in accordance with the nation included in the filename. At this stage, I had four Excel worksheets collectively pertaining to the 18 U.S.C. § 1030 charges filed against foreign actors from the four nations.

The FDD CCTI dataset was published on April 20, 2020 and does not appear to have been updated since the date of publication. Therefore, to compile cases of 18 U.S.C. § 1030 indictments that had been publicly announced by the DOJ after that date, I referred to news reports and consulted the "Justice News" database of the DOJ Office of Public Affairs. This database contains the DOJ's press releases, including those in which the DOJ announces indictments.

Finally, I consolidated the data by having each entry represent a § 1030 indictment, rather than an indicted individual.

3.7.4. Original Dataset of 18 U.S.C. § 1030 Bare Indictments

As a result of the data cleaning of the FDI CCTI dataset and the additional research to augment the cleaned data, I arrived at the following dataset, which forms the structural basis for my case study analysis. Each entry in the dataset is a publicized 18 U.S.C. § 1030 bare indictment issued against a national or nationals of China, North Korea, Iran, or Russia. "Publicization" refers to the date of the DOJ press release that publicly announced the 18 U.S.C. § 1030 indictment; since I theorize that the imposition of punishment's becoming common knowledge is the relevant public event that achieves the deterrent effect, I focus on the date of the press release rather than the date the indictment was issued. In accordance with legal style conventions, "Legal case name" includes only the

name of the first defendant named on the indictment, not the name of every defendant where multiple defendants are named. For the Chinese nationals, I included both the family name and given name of the lead defendant. There has been no evidence to indicate that any of the defendants are related to one another in a familial sense; if I were to list only the family name of the lead defendant, there would be a confusing overlap in the "Legal case name" values for disparate legal cases. The column entitled "#Δ" draws from the standard shorthand for 'number of defendants'; in legal practice, the Greek capital letter delta is often used to denote "defendant." If some of the defendants indicted in that indictment are not nationals of any of the four nations studied, those defendants were excluded from the defendant count.[12] The values under "Case study reference name" come from some feature of the respective legal case. For instance, "Mabna Institute case study" refers to the entity of which the defendants were alleged to be agents; "Lazarus case study" refers to the cyberattacking group of which the defendants were alleged to be a part; "Su Bin case study" refers to the name of the only defendant; "Equifax case study" refers to the name of the alleged victim of the cyberattacks described; and "SamSam Ransomware case study" refers to the malware that the defendants allegedly used to carry out their cyberattacks.

For ease of reference, I have assigned each entry a sequential "Code name." The prefixes are "XNA" for cases involving defendants who are Chinese nationals, "NK" for cases involving defendants who are North Korean nationals, and "IRAN" for cases involving

[12] For example, in the *U.S. v. Konovolov* indictment, there were ten defendants named; however, only five defendants were Russian nationals, so the "#Δ" value is coded as 5, not 10. In *U.S. v. Mohammadzadeh*, one of the two defendants is described as a "stateless national" (U.S. Attorney's Office, District of Massachusetts, September 15, 2020); as the other of the two defendants is an Iranian national, the "#Δ" value for this entry is coded as 1.

defendants who are Iranian nationals. "RUSS" is the prefix for cases involving defendants who are Russian nationals and whose alleged cyberattacks can be linked to the Russian government. "RNOST" denotes "Russian non-state" cases; these cases involve defendants who are Russian nationals, but there is no evidence to indicate that their alleged cyberattacks are linked to the Russian government. While a cyberattacker's level of governmental affiliation may lie on a spectrum, it is obvious that the indicted actors coded RNOST were not carrying out their alleged cyberattacks on behalf of the Russian government, so these cyberattacks would clearly lie at the low end of Healey's spectrum of nation-state responsibility. This is as opposed to accused cyberattackers of other countries such as China or Iran, in which the alleged cyberattacker's level of governmental affiliation is often debatable rather than obvious. Given that my theory does not turn on the alleged cyberattacker's precise level of governmental affiliation, the reason for presenting the Russian non-state actors in a separate category is that the large number of indicted and convicted Russian non-state actors is relevant for showing the additive effect of the *respondeat superior* principle's application. Considering the large number of similar cases, the details of most of these cases on Russian non-state actors can be grouped and discussed together.

I have sorted these entries by chronology. For the chronological ordering, the date used is the date that the indictment was publicly announced via DOJ press release. In some cases, the issuance of a bare indictment does not become publicly announced until apprehension of the actor against whom it was issued has occurred, which is to say – once the indictment was, in actuality, no longer "bare." As such, some of the DOJ press releases announce the arrest or sentencing of the indicted actor pursuant to charges of 18 U.S.C. §

1030. My rationale for basing the chronology on the date of public announcement rather than the date the bare indictment was filed is that, in accordance with CDT, the indictment can achieve only an extremely suboptimal deterrent effect if the presence of this purported deterrent measure is kept unknown to the public.

The following eight tables present the dataset. Table III is the complete dataset. Table IV is the dataset, but excluding the large number of entries coded RNOST. Tables V through IX present each of the five categories – RNOST, RUSS, XNA, NK, IRAN – separately. Finally, Table X is the complete dataset once again, with the entries color-coded by the nationality of the indicted individual(s).

The spreadsheets, in Excel file format, are also available for download alongside this paper. The Excel version available for separate download includes a column entitled "Press release URL," providing the link to a press release that publicizes the respective bare indictment.

TABLE III. CONSOLIDATED DATASET OF 18 U.S.C. § 1030 BARE INDICTMENTS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
RNOST-01	2012-01-17	Russia	*U.S. v. Zdorovenin*	2	Russian non-state actors case studies
RNOST-02	2013-01-23	Russia	*U.S. v. Kuzmin*	1	Russian non-state actors case studies
RNOST-03	2013-07-25	Russia	*U.S. v. Drinkman*	5	Russian non-state actors case studies
RNOST-04	2014-01-28	Russia	*U.S. v. Panin*	1	Russian non-state actors case studies
XNA-01	2014-05-19	China	*U.S. v. Wang Dong*	5	PLA Unit 61398 case study
RNOST-05	2014-06-02	Russia	*U.S. v. Bogachev*	1	Russian non-state actors case studies
RNOST-06	2014-07-07	Russia	*U.S. v. Seleznev*	1	Seleznev case study
XNA-02	2014-08-15	China	*U.S. v. Su Bin*	1	Su Bin case study
RNOST-07	2015-09-29	Russia	*U.S. v. Belorossov*	1	Russian non-state actors case studies
IRAN-01	2015-12-02	Iran	*U.S. v. Golestaneh*	1	Arrow Tech case study
IRAN-02	2016-03-24	Iran	*U.S. v. Fathi*	7	U.S. Financial Industry DDoS case study
RNOST-08	2016-10-21	Russia	*U.S. v. Nikulin*	1	Russian non-state actors case studies
RNOST-09	2017-03-14	Russia	*U.S. v. Vartanyan*	1	Russian non-state actors case studies
RUSS-01	2017-03-15	Russia	*U.S. v. Dokuchaev*	4	Yahoo case study
RNOST-10	2017-03-28	Russia	*U.S. v. Senakh*	1	Russian non-state actors case studies
RNOST-11	2017-05-21	Russia	*U.S. v. Levashov*	1	Russian non-state actors case studies
IRAN-03	2017-07-17	Iran	*U.S. v. Ajily*	2	Arrow Tech case study
IRAN-04	2017-11-21	Iran	*U.S. v. Mesri*	1	HBO case study
XNA-03	2017-11-27	China	*U.S. v. Wu Yingzhuo*	3	Boyusec case study
IRAN-05	2018-03-23	Iran	*U.S. v. Rafatnejad*	9	Mabna Institute case study
RUSS-02	2018-07-13	Russia	*U.S. v. Netyksho*	12	DNC/Clinton case study
RNOST-12	2018-07-27	Russia	*U.S. v. Malykhin*	1	Russian non-state actors case studies
RUSS-03	2018-10-04	Russia	*U.S. v. Morenets*	7	Anti-doping case study
XNA-04	2018-10-30	China	*U.S. v. Zhang Zhang-Gui*	10	JSSD case study
IRAN-06	2018-11-28	Iran	*U.S. v. Savandi*	2	SamSam Ransomware case study
XNA-05	2018-12-20	China	*U.S. v. Zhu Hua*	2	APT10 case study
IRAN-07	2019-02-13	Iran	*U.S. v. Witt*	4	Witt and Cyber Conspirators case study
XNA-06	2019-05-09	China	*U.S. v. Wang Fujie*	2	Anthem case study
RNOST-13	2019-05-16	Russia	*U.S. v. Konovolov*	5	Russian non-state actors case studies
RNOST-14	2019-05-29	Russia	*U.S. v. Bogdanov*	1	Russian non-state actors case studies
RNOST-15	2019-09-23	Russia	*U.S. v. Tyurin*	1	Russian non-state actors case studies
RNOST-16	2019-11-12	Russia	*U.S. v. Burkov*	1	Russian non-state actors case studies
RNOST-17	2019-12-05	Russia	*U.S. v. Yakubets*	2	Russian non-state actors case studies
XNA-07	2020-02-10	China	*U.S. v. Wu Zhiyong*	4	Equifax case study
XNA-08	2020-07-21	China	*U.S. v. Li Xiaoyu*	2	Two classmates case study
RNOST-18	2020-08-25	Russia	*U.S. v. Kriuchkov*	1	Russian non-state actors case studies
IRAN-08	2020-09-15	Iran	*U.S. v. Mohammadzadeh*	1	FBI new cyber policy case study
IRAN-09	2020-09-16	Iran	*U.S. v. Heidarian*	2	FBI new cyber policy case study
XNA-09	2020-09-16	China	*U.S. v. Zhang Haoran*	2	APT41 case study

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
XNA-10	2020-09-16	China	*U.S. v. Jiang Lizhi*	3	APT41 case study
IRAN-10	2020-09-17	Iran	*U.S. v. Arabi*	3	FBI new cyber policy case study
RUSS-04	2020-10-19	Russia	*U.S. v. Andrienko*	6	Sandworm case study
NK-01	2021-02-17	North Korea	*U.S. v. Jon*	3	Lazarus case study
RNOST-19	2021-06-16	Russia	*U.S. v. Koshkin*	1	Russian non-state actors case studies
XNA-11	2021-07-19	China	*U.S. v. Ding Xiaoyang*	4	APT40 case study
RNOST-20	2021-10-28	Russia	*U.S. v. Dunaev*	1	Russian non-state actors case studies
RNOST-21	2021-11-08	Russia	*U.S. v. Polyanin*	1	REvil case study
IRAN-11	2021-11-18	Iran	*U.S. v. Kazemi*	2	Kazemi and Kashian case study
RUSS-05	2022-03-24	Russia	*U.S. v. Akulov*	3	Energy infrastructure case study
RUSS-06	2022-03-24	Russia	*U.S. v. Gladkikh*	1	Energy infrastructure case study

TABLE IV. DATASET OF BARE INDICTMENTS, EXCLUDING RUSSIAN NON-STATE ACTORS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
XNA-01	2014-05-19	China	*U.S. v. Wang Dong*	5	PLA Unit 61398 case study
XNA-02	2014-08-15	China	*U.S. v. Su Bin*	1	Su Bin case study
IRAN-01	2015-12-02	Iran	*U.S. v. Golestaneh*	1	Arrow Tech case study
IRAN-02	2016-03-24	Iran	*U.S. v. Fathi*	7	U.S. Financial Industry DDoS case study
RUSS-01	2017-03-15	Russia	*U.S. v. Dokuchaev*	4	Yahoo case study
IRAN-03	2017-07-17	Iran	*U.S. v. Ajily*	2	Arrow Tech case study
IRAN-04	2017-11-21	Iran	*U.S. v. Mesri*	1	HBO case study
XNA-03	2017-11-27	China	*U.S. v. Wu Yingzhuo*	3	Boyusec case study
IRAN-05	2018-03-23	Iran	*U.S. v. Rafatnejad*	9	Mabna Institute case study
RUSS-02	2018-07-13	Russia	*U.S. v. Netyksho*	12	DNC/Clinton case study
RUSS-03	2018-10-04	Russia	*U.S. v. Morenets*	7	Anti-doping case study
XNA-04	2018-10-30	China	*U.S. v. Zhang Zhang-Gui*	10	JSSD case study
IRAN-06	2018-11-28	Iran	*U.S. v. Savandi*	2	SamSam Ransomware case study
XNA-05	2018-12-20	China	*U.S. v. Zhu Hua*	2	APT10 case study
IRAN-07	2019-02-13	Iran	*U.S. v. Witt*	4	Witt and Cyber Conspirators case study
XNA-06	2019-05-09	China	*U.S. v. Wang Fujie*	2	Anthem case study
XNA-07	2020-02-10	China	*U.S. v. Wu Zhiyong*	4	Equifax case study
XNA-08	2020-07-21	China	*U.S. v. Li Xiaoyu*	2	Two classmates case study
IRAN-08	2020-09-15	Iran	*U.S. v. Mohammadzadeh*	1	FBI new cyber policy case study
IRAN-09	2020-09-16	Iran	*U.S. v. Heidarian*	2	FBI new cyber policy case study
XNA-09	2020-09-16	China	*U.S. v. Zhang Haoran*	2	APT41 case study
XNA-10	2020-09-16	China	*U.S. v. Jiang Lizhi*	3	APT41 case study
IRAN-10	2020-09-17	Iran	*U.S. v. Arabi*	3	FBI new cyber policy case study
RUSS-04	2020-10-19	Russia	*U.S. v. Andrienko*	6	Sandworm case study
NK-01	2021-02-17	North Korea	*U.S. v. Jon*	3	Lazarus case study
XNA-11	2021-07-19	China	*U.S. v. Ding Xiaoyang*	4	APT40 case study
IRAN-11	2021-11-18	Iran	*U.S. v. Kazemi*	2	Kazemi and Kashian case study
RUSS-05	2022-03-24	Russia	*U.S. v. Akulov*	3	Energy infrastructure case study
RUSS-06	2022-03-24	Russia	*U.S. v. Gladkikh*	1	Energy infrastructure case study

TABLE V. 18 U.S.C. § 1030 INDICTMENTS OF RUSSIAN NON-STATE ACTORS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
RNOST-01	2012-01-17	Russia	*U.S. v. Zdorovenin*	2	Russian non-state actors case studies
RNOST-02	2013-01-23	Russia	*U.S. v. Kuzmin*	1	Russian non-state actors case studies
RNOST-03	2013-07-25	Russia	*U.S. v. Drinkman*	5	Russian non-state actors case studies
RNOST-04	2014-01-28	Russia	*U.S. v. Panin*	1	Russian non-state actors case studies
RNOST-05	2014-06-02	Russia	*U.S. v. Bogachev*	1	Russian non-state actors case studies
RNOST-06	2014-07-07	Russia	*U.S. v. Seleznev*	1	Seleznev case study
RNOST-07	2015-09-29	Russia	*U.S. v. Belorossov*	1	Russian non-state actors case studies
RNOST-08	2016-10-21	Russia	*U.S. v. Nikulin*	1	Russian non-state actors case studies
RNOST-09	2017-03-14	Russia	*U.S. v. Vartanyan*	1	Russian non-state actors case studies
RNOST-10	2017-03-28	Russia	*U.S. v. Senakh*	1	Russian non-state actors case studies
RNOST-11	2017-05-21	Russia	*U.S. v. Levashov*	1	Russian non-state actors case studies
RNOST-12	2018-07-27	Russia	*U.S. v. Malykhin*	1	Russian non-state actors case studies
RNOST-13	2019-05-16	Russia	*U.S. v. Konovolov*	5	Russian non-state actors case studies
RNOST-14	2019-05-29	Russia	*U.S. v. Bogdanov*	1	Russian non-state actors case studies
RNOST-15	2019-09-23	Russia	*U.S. v. Tyurin*	1	Russian non-state actors case studies
RNOST-16	2019-11-12	Russia	*U.S. v. Burkov*	1	Russian non-state actors case studies
RNOST-17	2019-12-05	Russia	*U.S. v. Yakubets*	2	Russian non-state actors case studies
RNOST-18	2020-08-25	Russia	*U.S. v. Kriuchkov*	1	Russian non-state actors case studies
RNOST-19	2021-06-16	Russia	*U.S. v. Koshkin*	1	Russian non-state actors case studies
RNOST-20	2021-10-28	Russia	*U.S. v. Dunaev*	1	Russian non-state actors case studies
RNOST-21	2021-11-08	Russia	*U.S. v. Polyanin*	1	REvil case study

TABLE VI. 18 U.S.C. § 1030 INDICTMENTS OF RUSSIAN NATIONALS, EXCLUDING NON-STATE ACTORS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
RUSS-01	2017-03-15	Russia	*U.S. v. Dokuchaev*	4	Yahoo case study
RUSS-02	2018-07-13	Russia	*U.S. v. Netyksho*	12	DNC/Clinton case study
RUSS-03	2018-10-04	Russia	*U.S. v. Morenets*	7	Anti-doping case study
RUSS-04	2020-10-19	Russia	*U.S. v. Andrienko*	6	Sandworm case study
RUSS-05	2022-03-24	Russia	*U.S. v. Akulov*	3	Energy infrastructure case study
RUSS-06	2022-03-24	Russia	*U.S. v. Gladkikh*	1	Energy infrastructure case study

TABLE VII. 18 U.S.C. § 1030 INDICTMENTS OF CHINESE NATIONALS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
XNA-01	2014-05-19	China	*U.S. v. Wang Dong*	5	PLA Unit 61398 case study
XNA-02	2014-08-15	China	*U.S. v. Su Bin*	1	Su Bin case study
XNA-03	2017-11-27	China	*U.S. v. Wu Yingzhuo*	3	Boyusec case study
XNA-04	2018-10-30	China	*U.S. v. Zhang Zhang-Gui*	10	JSSD case study
XNA-05	2018-12-20	China	*U.S. v. Zhu Hua*	2	APT10 case study
XNA-06	2019-05-09	China	*U.S. v. Wang Fujie*	2	Anthem case study
XNA-07	2020-02-10	China	*U.S. v. Wu Zhiyong*	4	Equifax case study
XNA-08	2020-07-21	China	*U.S. v. Li Xiaoyu*	2	Two classmates case study
XNA-09	2020-09-16	China	*U.S. v. Zhang Haoran*	2	APT41 case study
XNA-10	2020-09-16	China	*U.S. v. Jiang Lizhi*	3	APT41 case study
XNA-11	2021-07-19	China	*U.S. v. Ding Xiaoyang*	4	APT40 case study

TABLE VIII. 18 U.S.C. § 1030 INDICTMENTS OF NORTH KOREAN NATIONALS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
NK-01	2021-02-17	North Korea	*U.S. v. Jon*	3	Lazarus case study

TABLE IX. 18 U.S.C. § 1030 INDICTMENTS OF IRANIAN NATIONALS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
IRAN-01	2015-12-02	Iran	*U.S. v. Golestaneh*	1	Arrow Tech case study
IRAN-02	2016-03-24	Iran	*U.S. v. Fathi*	7	U.S. Financial Industry DDoS case study
IRAN-03	2017-07-17	Iran	*U.S. v. Ajily*	2	Arrow Tech case study
IRAN-04	2017-11-21	Iran	*U.S. v. Mesri*	1	HBO case study
IRAN-05	2018-03-23	Iran	*U.S. v. Rafatnejad*	9	Mabna Institute case study
IRAN-06	2018-11-28	Iran	*U.S. v. Savandi*	2	SamSam Ransomware case study
IRAN-07	2019-02-13	Iran	*U.S. v. Witt*	4	Witt and Cyber Conspirators case study
IRAN-08	2020-09-15	Iran	*U.S. v. Mohammadzadeh*	1	FBI new cyber policy case study
IRAN-09	2020-09-16	Iran	*U.S. v. Heidarian*	2	FBI new cyber policy case study
IRAN-10	2020-09-17	Iran	*U.S. v. Arabi*	3	FBI new cyber policy case study
IRAN-11	2021-11-18	Iran	*U.S. v. Kazemi*	2	Kazemi and Kashian case study

TABLE X. COLOR-CODED, CONSOLIDATED DATASET OF 18 U.S.C. § 1030 BARE INDICTMENTS

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
RNOST-01	2012-01-17	Russia	*U.S. v. Zdorovenin*	2	Russian non-state actors case studies
RNOST-02	2013-01-23	Russia	*U.S. v. Kuzmin*	1	Russian non-state actors case studies
RNOST-03	2013-07-25	Russia	*U.S. v. Drinkman*	5	Russian non-state actors case studies
RNOST-04	2014-01-28	Russia	*U.S. v. Panin*	1	Russian non-state actors case studies
XNA-01	2014-05-19	China	*U.S. v. Wang Dong*	5	PLA Unit 61398 case study
RNOST-05	2014-06-02	Russia	*U.S. v. Bogachev*	1	Russian non-state actors case studies
RNOST-06	2014-07-07	Russia	*U.S. v. Seleznev*	1	Seleznev case study
XNA-02	2014-08-15	China	*U.S. v. Su Bin*	1	Su Bin case study
RNOST-07	2015-09-29	Russia	*U.S. v. Belorossov*	1	Russian non-state actors case studies
IRAN-01	2015-12-02	Iran	*U.S. v. Golestaneh*	1	Arrow Tech case study
IRAN-02	2016-03-24	Iran	*U.S. v. Fathi*	7	U.S. Financial Industry DDoS case study
RNOST-08	2016-10-21	Russia	*U.S. v. Nikulin*	1	Russian non-state actors case studies
RNOST-09	2017-03-14	Russia	*U.S. v. Vartanyan*	1	Russian non-state actors case studies
RUSS-01	2017-03-15	Russia	*U.S. v. Dokuchaev*	4	Yahoo case study
RNOST-10	2017-03-28	Russia	*U.S. v. Senakh*	1	Russian non-state actors case studies
RNOST-11	2017-05-21	Russia	*U.S. v. Levashov*	1	Russian non-state actors case studies
IRAN-03	2017-07-17	Iran	*U.S. v. Ajily*	2	Arrow Tech case study
IRAN-04	2017-11-21	Iran	*U.S. v. Mesri*	1	HBO case study
XNA-03	2017-11-27	China	*U.S. v. Wu Yingzhuo*	3	Boyusec case study
IRAN-05	2018-03-23	Iran	*U.S. v. Rafatnejad*	9	Mabna Institute case study
RUSS-02	2018-07-13	Russia	*U.S. v. Netyksho*	12	DNC/Clinton case study
RNOST-12	2018-07-27	Russia	*U.S. v. Malykhin*	1	Russian non-state actors case studies
RUSS-03	2018-10-04	Russia	*U.S. v. Morenets*	7	Anti-doping case study
XNA-04	2018-10-30	China	*U.S. v. Zhang Zhang-Gui*	10	JSSD case study
IRAN-06	2018-11-28	Iran	*U.S. v. Savandi*	2	SamSam Ransomware case study
XNA-05	2018-12-20	China	*U.S. v. Zhu Hua*	2	APT10 case study
IRAN-07	2019-02-13	Iran	*U.S. v. Witt*	4	Witt and Cyber Conspirators case study
XNA-06	2019-05-09	China	*U.S. v. Wang Fujie*	2	Anthem case study
RNOST-13	2019-05-16	Russia	*U.S. v. Konovolov*	5	Russian non-state actors case studies
RNOST-14	2019-05-29	Russia	*U.S. v. Bogdanov*	1	Russian non-state actors case studies
RNOST-15	2019-09-23	Russia	*U.S. v. Tyurin*	1	Russian non-state actors case studies
RNOST-16	2019-11-12	Russia	*U.S. v. Burkov*	1	Russian non-state actors case studies
RNOST-17	2019-12-05	Russia	*U.S. v. Yakubets*	2	Russian non-state actors case studies
XNA-07	2020-02-10	China	*U.S. v. Wu Zhiyong*	4	Equifax case study
XNA-08	2020-07-21	China	*U.S. v. Li Xiaoyu*	2	Two classmates case study
RNOST-18	2020-08-25	Russia	*U.S. v. Kriuchkov*	1	Russian non-state actors case studies
IRAN-08	2020-09-15	Iran	*U.S. v. Mohammadzadeh*	1	FBI new cyber policy case study
IRAN-09	2020-09-16	Iran	*U.S. v. Heidarian*	2	FBI new cyber policy case study
XNA-09	2020-09-16	China	*U.S. v. Zhang Haoran*	2	APT41 case study

Code name	Publicization	Nationality of Δ(s)	Legal case name	#Δ	Case study reference name
XNA-10	2020-09-16	China	*U.S. v. Jiang Lizhi*	3	APT41 case study
IRAN-10	2020-09-17	Iran	*U.S. v. Arabi*	3	FBI new cyber policy case study
RUSS-04	2020-10-19	Russia	*U.S. v. Andrienko*	6	Sandworm case study
NK-01	2021-02-17	North Korea	*U.S. v. Jon*	3	Lazarus case study
RNOST-19	2021-06-16	Russia	*U.S. v. Koshkin*	1	Russian non-state actors case studies
XNA-11	2021-07-19	China	*U.S. v. Ding Xiaoyang*	4	APT40 case study
RNOST-20	2021-10-28	Russia	*U.S. v. Dunaev*	1	Russian non-state actors case studies
RNOST-21	2021-11-08	Russia	*U.S. v. Polyanin*	1	REvil case study
IRAN-11	2021-11-18	Iran	*U.S. v. Kazemi*	2	Kazemi and Kashian case study
RUSS-05	2022-03-24	Russia	*U.S. v. Akulov*	3	Energy infrastructure case study
RUSS-06	2022-03-24	Russia	*U.S. v. Gladkikh*	1	Energy infrastructure case study

3.8. Summary of Argument; Case Study Organization

Overall, then, I argue that bare indictments deter cyberattacks because the publicization of a bare indictment makes common knowledge the label of "criminal outcast"; the imposition of this label triggers a package of informal sanctions. Among this package of informal sanctions, an attack to face directly undermines status-seeking objectives, and practical consequences indirectly outweigh thrill-seeking objectives. In accordance with the principle of *respondeat superior*, this attack to face can be imputable against the nation-state of which the indicted individuals are nationals. Considering that nation-states often care about their status among the global hierarchy of the international community and criminal misconduct can be conceptualized as the worst form of misconduct, a nation-state against whom the attack on national face is imputable will be sensitive to any applicable deterrent effects stemming from *criminal* naming-and-shaming, as opposed to civil naming-and-shaming.

In proving the six hypotheses, the body chapters are organized as follows. Chapter 4 presents case studies to prove **H1**, **H2**, and **H3**, which are the core hypotheses relating to the deterrent mechanism of bare indictments. The lead case study is the PLA Unit 61398 case study, in which China – a prestige-seeking nation-state actor – was deterred by bare indictment. Since **H6** – the hypothesized shift toward profit-seeking – is based on the combined mechanistic effect of the core hypotheses, Chapter 4 also demonstrates a trend toward profit-seeking motives over time. **H4** is an underlying hypothesis that explains why the nation-state government may issue an indignant public response even though the nation-state is never a named defendant. As the closing case of Chapter 4 regards the

contrast between civil naming-and-shaming versus criminal naming-and-shaming, it calls to light the nature of the attack to face that underlies both **H1** and **H5**.

This transitions to Chapter 5, in which the case study analysis exclusively regards Russian cases and concentrates on supporting **H5**; this is the hypothesis regarding nation-state responses to the imputed attack to national face. To prove **H5**, I show that bare indictment would not have deterred the profit-seeking objectives of the numerous indicted Russian non-state actors, yet I argue that the numerous indictments of these subsequently convicted profit-seeking nonstate actors so embarrassed the Russian state that the Russian government was prompted to make preemptive high-profile arrests of its own nationals, to whom the Colonial Pipeline cyberattack had been technically attributed.

Chapter 6 regards other aspects of bare indictments, examining two Iranian cases wherein the deterrent result was not as would be predicted by the theory. This chapter explains what underlying or intervening factors were responsible for the unexpected results. In the first of Chapter 6's case studies, I argue that deterrence was achieved, irrespective of the actors' motive, due to the heightened risk of apprehension as well as the risk of *formal* punishment; in the second, I argue that the counterproductive and simultaneous imposition of duplicative economic sanctions meant that deterrence against status-seeking actors was *not* achieved as would have been predicted. Thus, I suggest that further understanding of bare indictments' deterrent effect can be achieved through examining these counterexamples.

Any counterarguments are usually raised and addressed within the case study analyses. Many of the counterarguments that have been raised by other scholars speak to

competing interpretations of particular case studies, rather than against my theory at large. Moreover, as mentioned before, the features of some case studies may be better suited than are those of other case studies for providing examples to rebut the relevant counterarguments.

The following Table XI summarizes the hypotheses, their corresponding predictions, and the case studies my project will analyze to provide evidence in support of each hypothesis.

TABLE XI. HYPOTHESES, PREDICTIONS, AND EVIDENCE

Hypothesis	***Prediction***	***Case study evidence***
H1: Bare indictments are likely to deter status-seeking cyberattacks, because the attack on face in the package of informal sanctions triggered by bare indictment tends to directly undermine the adversary's expected benefit of status; these informal sanctions can lower *B* such that *(PC)(C)* is likely to exceed *(PB)(B)*.	**P1**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by status-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.	In the PLA Unit 61398 case study [XNA-01], Chinese cyberattacking activity dramatically declined after the publicization of a bare indictment against prestige-seeking cyberattacks. In the U.S. Financial Industry DDoS attacks case study [IRAN-02], SDT would have predicted that the dominance-seeking cyberattacks would escalate, yet the cyberattacks did not continue after the publicization of a bare indictment.
H2: Bare indictments are likely to deter thrill-seeking cyberattacks, because the practical consequences in the package of informal sanctions triggered by bare indictment tend to indirectly outweigh the adversary's expected benefit of emotional thrill; these informal sanctions can raise PC and / or raise *C* such that *(PC)(C)* is likely to exceed *(PB)(B)*.	**P2**: When a bare indictment is issued against an alleged cyberattacker primarily motivated by thrill-seeking, indicia of deterrent effects will likely be observable shortly after the publicization of that bare indictment.	In the SamSam Ransomware case study [IRAN-06], the thrill-seeking cyberattacks attributable to the indicted actors came to an abrupt halt immediately after the publicization of a bare indictment.
H3: Bare indictments are unlikely to deter profit-seeking cyberattacks, because the package of informal sanctions triggered by bare indictment is neither likely to directly undermine nor likely to indirectly outweigh the adversary's expected benefit of monetary profit.	**P3**: No indicia of deterrent effects will likely be observable after the publicization of a bare indictment issued against an alleged cyberattacker primarily motivated by profit-seeking.	In the Lazarus case study [NK-01], the profit-seeking cyberattacks continued even after the publicization of a bare indictment.

Hypothesis	*Prediction*	*Case study evidence*
H4: The deterrent effect of a bare indictment issued against an alleged cyberattacker will tend to be applicable against that alleged cyberattacker's foreign nation-state in accordance with the principle of *respondeat superior*.	**P4**: Even though the nation-state itself is not a named defendant, the nation-state government may issue an indignant public statement in response to a bare indictment of individuals alleged to be cyberattacking on the nation-state's behalf.	The indicted individuals' nation-state government issued an indignant public response in cases including the PLA Unit 61398 case study [XNA-01], involving a bare indictment against arguably prestige-seeking officers of the Chinese military.
H5: Given that many nation-states care about national status, nation-states against whom bare indictments are imputable will be sensitive to the applicable deterrent effects of the "criminal naming-and-shaming" attack on face that bare indictments achieve.	**P5**: When a publicized bare indictment is applicable against a nation-state that cares about national status, the nation-state will likely react by attempting to recover status.	Following numerous bare indictments issued against Russian profit-seeking actors, the Russian government preemptively arrested the Colonial Pipeline profit-seeking suspected cyberattackers before a U.S. bare indictment was issued against them.
H6: When bare indictments are issued against suspected cyberattackers and publicized, then over time cyberattacks will shift toward being motivated by profit-seeking.	**P6**: Over time, publicized bare indictments will come to be issued almost exclusively against cyberattacks that are motivated by profit-seeking.	The indictments in case studies [XNA-02] through [XNA-10] and in case studies [IRAN-07] through [IRAN-11] are representative of a gradual shift toward profit-seeking.

CHAPTER 4

PROVING THE THEORY:

WHY BARE INDICTMENTS CAN DETER CYBERATTACKS

4.0. Chapter Overview: The Core Theory on Why Bare Indictments Deter Cyberattacks

This chapter examines case studies that demonstrate the core aspects of the theory on bare indictments' deterrent effect. First, Section 4.1. contextualizes status-seeking by conducting a foreign policy analysis that reveals what the Chinese state conceives of as markers of prestige. The next three sections regard cases on – respectively – status-seeking, profit-seeking, and thrill-seeking. Section 4.2. covers the primary case study: the May 19, 2014 bare indictment of five Chinese army officers. In this case study, I analyze data on Chinese cyberattacking activity to prove that the bare indictment achieved a deterrent effect against Chinese cyberattacks. Section 4.3. shows why profit-seeking motives meant that the North Korean state-sponsored Lazarus Group was undeterred by bare indictment. As for the discussion of thrill-seeking, I show in Section 4.4. that the publicization of a bare indictment brought a campaign of thrill-seeking cyberattacks to an immediate halt.

Section 4.5. is comprised of brief case studies of nine further bare indictments issued against Chinese nationals for alleged violations of 18 U.S.C. § 1030. I find that these nine bare indictments are representative of a shift away from prestige-seeking cyberattacks and toward profit-seeking cyberattacks; this provides evidence that aligns with the prediction on observable trends that would be generated if bare indictments were to achieve a general deterrent effect. Section 4.6. explores a similar trend toward profit-

seeking, as is demonstrated in bare indictments issued against Iranian nationals since 2019. This section also discusses a case study that provides an empirical example to illustrate the foundational theoretical assumption that a given cyberattacker can shift motives over time. Section 4.7. examines a 2021 bare indictment that the U.S. announced in conjunction with the coordinated actions of an international coalition. I use this case study to further explore why the criminal rather than civil nature of bare indictments in diplomatic communication plays an integral role in bare indictments' effectiveness as a deterrent measure.

4.1. The Primacy of Scientific Advancement and Business Development as Markers of Prestige in China's Domestic and Foreign Policy

To analyze the motives of Chinese cyberattackers, it is necessary to understand what the Chinese state considers markers of prestige. With an understanding of what Chinese leaders believe will demonstrate prestige for China as a nation-state, the argument can be made that cyberattacks that might initially appear to be primarily motivated by profit-seeking are better characterizable as prestige-seeking based on the qualitative nature of the targeted data when read in context with Chinese indicia of prestige. When determining prestige-seeking motives in cyberattacks allegedly perpetrated by Chinese nation-state actors, there are two essential propositions to keep in mind. One, China's foreign policy goals center on prestige. Two, China considers scientific advancement and business development to be markers of prestige.

Scholars are in consensus about the primacy of prestige in China's foreign policy. Among analysts of contemporary Chinese policy, "China's strategy to gain international prestige" is well established; for instance, Filip Viskupič characterizes China's prestige-seeking strategy as "the cornerstone of [China's] foreign policy" (Viskupič 2021, 1). Similarly, the opening lines of Andrew Erickson's 2019 analysis present the contention as nearly indisputable: "To the extent that any nation has a grand strategy, China surely does. The vision is no secret: Xi Jinping vows to make China great again" (Erickson 2019). China's deeply rooted policy emphasis on prestige stretches back hundreds of years, far predating the era of cyberattacks. Erickson's analysis, like those of Deborah Welch Larson and Alexei Shevchenko (2019) and Yuen Foong Khong (2019), presents prestige-seeking as a longstanding strategy rooted in China's self-perception as a former great power brought low by foreign colonial occupation in what has been termed the "Century of Humiliation" from approximately 1839 to 1949 (Tischler 2020). Prestige-seeking, a strategy arguably driven by a fear of further humiliation, has become particularly prominent since Chinese President Xi Jinping took office in 2013. For example, Erickson cites a 2017 address to the National Congress of the Communist Party of China, in which Xi alludes to China's history of humiliation and sets out a direction for the future of the state: "The Chinese nation, which since modern times began had endured so much for so long, has achieved a tremendous transformation: it has stood up, grown rich, and is becoming strong" (Xi 2017).

With prestige being China's overarching foreign policy goal, looking to Chinese national policy documents and speeches – in particular, China's 2011-2015 "Five Year Plan" and Xi's 2017 address – indicates that, amidst the advent of cyberattacks, two matters that the Chinese state has positioned as markers of prestige are scientific advancement and

business development. In English translation, Part I of China's 2011-2015 "Five Year Plan" – a document of national policy prepared by the Chinese government (Casey and Koleski 2011) – starts the document with a focus on "scientific development": "The theme of scientific development is required by the times" (China's National People's Congress 2011, Ch. 2). The opening sections also show that scientific advancement and business development are intertwined: "The inevitable way to promote scientific development is to maintain the cardinal line of speeding up the transformation of economic development" (China's National People's Congress 2011, Ch. 2). The Chinese state not only positions economic development as supporting scientific advancement, but also presents the two as mutually reinforcing: "Scientific progress and innovation will support the transformation [of economic development]" (China's National People's Congress 2011, Ch. 2). Moreover, Chapter 15 of the 2011-2015 Five Year Plan further describes that the development of a thriving business environment is necessary to "promote scientific innovation" (China's National People's Congress 2011, Ch. 15). Near the beginning of his 2017 address, Xi emphasized the interconnection of scientific advancement and economic advancement in promoting China's prestige. Xi reviewed the Chinese state's progress of the "past five years," highlighting the importance of China's "major achievements in economic development" in supporting scientific advancement: "Through devoting great energy to implementing the innovation-driven development strategy, we have seen much accomplished toward making China a country of innovators, with major advances made in science and technology" (Xi 2017, 1-2). On page 26 of the English translation of Xi's speech, Xi again used the "country of innovators" phrasing to further present scientific advancement and business development as sources of Chinese national prestige (Xi 2017,

26). Saying "Innovation is the primary driving force behind development," Xi pushed for "national innovation" as a means of raising China's status in the international order, as he stated, "We should cultivate a large number of *world-class* scientists [emphasis added]" (Xi 2017, 26). As this 2011 official Chinese policy document and this 2017 speech from China's head of state each emphasize the importance of national scientific advancement and business development in furtherance of China's prestige-centered foreign policy, this textual evidence supports the argument that China sees scientific advancement and business development as markers of prestige. Correspondingly, whenever cyberattacks thought to be perpetrated by Chinese nation-state actors target data that could directly be utilized for scientific advancement, business development, or both, then the argument can be made that these cyberattacks were primarily motivated by prestige-seeking.

4.2.0. Bare Indictments Frustrate Prestige-Seeking Objectives of Chinese State-Sponsored Cyberattackers [XNA-01]

On May 19, 2014, the Office of Public Affairs ("OPA") of the U.S. Department of Justice ("DOJ") publicly announced the unsealing of the U.S.'s first federal criminal indictment alleging violations of 18 U.S.C. § 1030 by foreign nation-state actors (DOJ OPA, May 19, 2014). The indictment alleged that the five defendants were members of Unit 61398 of the Chinese People's Liberation Army ("PLA"), implying that these five Chinese nationals executed their cyberattacks on behalf of the Chinese state.

Just as the U.S. used a press release to announce the indictment's unsealing, China's immediate and indignant response was made via the medium of public statement. In remarks circulated globally on May 20, 2014, Spokesperson Qin Gang of the Chinese

Foreign Ministry called the U.S.'s enforcement of 18 U.S.C. § 1030 against China improper, a "[gross violation of] the basic norms governing international relations" (Qin 2014). One year later, however, U.S. President Barack Obama and Chinese President Xi Jinping signed a cooperative agreement promising that neither the U.S. nor China would engage in or condone cyberattacking "with the intent of providing competitive advantages to companies or commercial sectors" (White House 2015). Was the agreement indicative of a deterrence success engendered by the issuance of a bare indictment, or – as some analysts have argued – does the totality of the evidence point to a deterrence failure?

Even though evidence has emerged that would support the contention of a deterrence success, it remains to be established that the bare indictment rather than some other cause was responsible for a deterrent effect against cyberattacks perpetrated by Chinese nationals; moreover, the mechanistic reasons why the bare indictment could be responsible for any deterrent effect remain unexplained. Legal journalist Benjamin Wittes suggested that if "a dropoff in IP [intellectual property] theft cases emanating from China" were subsequently observed, that drop would be evidence of a deterrent effect (Wittes, October 05, 2015). However, even after evidence emerged of a sharp drop in cyberattacking activity from China (Mandiant 2016), some scholars have pointed out that this does not prove causality (Keitner 2019, 208), since other intervening causes could be responsible for the decline (Goldsmith 2016). Responding to early reports that seemed to indicate a dramatic decline in Chinese cyberattacking activity following the PLA Unit 61398 indictment, Wittes acknowledged the reported decline, but wrote that the reason why indictments could have achieved this decline was unclear: "I'm honestly not sure why these

indictments so bother Chinese officialdom. They wouldn't have particularly bothered me had I been in their shoes" (Wittes, December 01, 2015).

This section aims to provide answers to these unexplained features and outcomes of the PLA Unit 61398 case. I argue not only that this bare indictment was successful in achieving specific and general deterrence against cyberattacks linked to the Chinese state, but also that the deterrent effect was not merely anomalous; this case study is demonstrative of the mechanistic process by which bare indictments can serve as an optimal deterrent measure. To more precisely determine what aspects of bare indictments can achieve a deterrent effect upon the cyber adversaries against which they are issued, this subsection examines this earliest case of the U.S.'s indictments alleging violations of 18 U.S.C. § 1030 by a foreign nation-state actor. I analyze the information presented in the press release and the indictment – in context with the surrounding circumstances of the case – to argue that the allegedly state-sponsored cyberattackers' motives were primarily prestige-seeking. Next, I analyze why the Chinese state spokesperson's public response evidences that the label of criminalization is imputable to the nation-state that evidently must have ordered the indicted officers' alleged cyberattacks. I review the literature and examine the data on the Chinese state's changed behavior to conclude that the indictment did indeed deter the Chinese state from mounting further cyberattacks. Then, to delineate the contours of the bare indictment mechanism, I compare this project's theory with other scholars' explanations. In the debate over the deterrent effect of bare indictments, scholars have suggested that the constituent functions of bare indictments, particularly the technical attribution function or what has been referred to as the "name-and-shame" function, are responsible for deterring cyberattackers. To show that the labeling mechanism better

explains the deterrent effect of bare indictments than do either of these other constituent functions, I call attention to two events in which each of these two functions was respectively deployed against the Chinese state in response to the attacks allegedly perpetrated by PLA Unit 61398. Despite these constituent functions being carried out more effectively via alternative policy tools than would have been attained by bare indictment, technical attribution and naming-and-shaming each failed to have a deterrent effect when deployed via policy tools other than domestic criminal charges. Overall, then, I show that naming-and-shaming alone is unlikely to achieve any deterrent effects, but the *public, criminal* naming-and-shaming quality of the attack to face can achieve a deterrent effect against prestige-seeking cyberattackers by criminalizing them. This case study supports the argument that the deterrent effect of bare indictments is driven by bare indictments' features as a unique policy instrument. Thus, I use the PLA Unit 61398 case study to offer theory-building evidence for the hypothesis that bare indictments deter cyberattackers because they label the indicted actors "criminal outcasts," which triggers a package of informal sanctions that directly frustrates the objective of prestige-seeking actors – even when those alleged cyberattackers are military officers backed by the resources of a nation-state.

4.2.1. The Prestige-Seeking Motives of PLA Unit 61398's Alleged Cyberattacks

The allegations in the indictment, when interpreted in the context of China's foreign policy goals, show that the cyberattackers were primarily prestige-seeking. Upon cursory examination, the nature of the criminal charges might lead one to believe that the

perpetrators of the cyberattacks were primarily motivated by profit-seeking. For instance, the press release states that all five of the Chinese nationals were charged under 18 U.S.C. § 1030(c)(2)(B)(i), which is "Accessing (or attempting to access) a protected computer without authorization to obtain information *for the purpose of commercial advantage and private financial gain* [emphasis added]" (DOJ OPA, May 19, 2014). However, a closer look at the data targeted by these cyberattacks reveals that the cyberattackers' objectives resonate with China's prestige-seeking policy goals. As discussed in Section 4.1., the Chinese state positions scientific advancement and business development as means of gaining prestige. Here, the indictment alleges that the five defendants used unauthorized access to take "proprietary and confidential technical and design specifications" from the U.S. energy firm Westinghouse (*Wang Dong* indictment, 2). This taking of design specifications is clearly related to scientific advancement, and hence is arguably reflective of prestige-seeking on behalf of the Chinese state. In its description of other offenses, the indictment itself connects cyber thefts of information with the policy goals of Chinese state-owned business enterprises. The indictment alleges that these members used violations of 18 U.S.C. § 1030 to obtain thousands of email messages regarding internal business strategy discussions of U.S. firms that, tellingly, were contemporaneously involved in litigation against Chinese firms (*Wang Dong* indictment, 5). Given the Chinese state's emphasis on scientific advancement and business development as means of gaining prestige, looking to the directly scientific- and business-related information that these members of PLA Unit 61398 allegedly targeted via cyberattacks supports the contention that these cyberattacks were primarily motivated by prestige-seeking on behalf of the Chinese state.

Moreover, what the Chinese government sees as markers of national prestige can be straightforwardly imputed to the accused PLA Unit 61398 officers; their role as Chinese military officers leads to the presumption that they were agents of the Chinese government, allegedly carrying out prestige-seeking cyberattacks on behalf of China. The application of the *respondeat superior* principle also explains why the Chinese state saw fit to respond at all. Since the publicization of the bare indictment made common knowledge the U.S.'s attack on China's national face, China issued a public statement denying the bare indictment's insinuation that the Chinese state had engaged in criminality.

4.2.2. China's Denial of Criminality; The Limited Norm-Setting of the 2015 Cyber Agreement between Xi and Obama

The Chinese state spokesperson's swift, indignant public response indicates that China saw the bare indictment as a threat to its status in the social hierarchy of the international community. Just as the U.S. publicized the bare indictment against the PLA Unit 61398 officers, China made its response to the bare indictment common knowledge through public circulation. Analysis of Qin's public statement, particularly its lack of direct denial and its invocation of the social norms of the global order, supports the argument that what "so [bothered] Chinese officialdom" (Wittes, December 01, 2015) about the bare indictment was the U.S.'s public accusation of criminality.

On May 20, 2014, the day after the DOJ announced the bare indictment against the PLA Unit 61398 officers, Spokesperson Qin Gang of the Chinese Foreign Ministry issued public remarks entitled "China Reacts Strongly to US Announcement of Indictment Against

Chinese Personnel." The title itself indicates a reason why the Chinese state saw fit to issue a public response: China was not "[reacting] strongly" to the indictment itself, but rather, the public "announcement" of the indictment. This suggests that China's concern was over how the nation would be viewed in the eyes of others, and that China saw the indictment's announcement as a threat to its global status.

Qin asserted that the criminal indictment itself was invalid in having been "based on deliberately fabricated facts" (Qin 2014). However, Qin did not provide any information or evidence to directly refute the accusations in the indictment. Instead, Qin gave only a general denial: "The Chinese government, the Chinese military and their relevant personnel have never engaged or participated in cyber theft of trade secrets" (Qin 2014). Qin's failure to directly refute the U.S. criminal charges suggests that the Chinese state did not have factual grounds to directly refute the U.S. charges against its officers.

Toward the beginning of Qin's remarks, Qin had called the U.S.'s enforcement of 18 U.S.C. § 1030 against China improper, a "[gross violation of] the basic norms governing international relations" (Qin 2014). Indeed, most of Qin's response focused not on denying the accusations, but on repositioning the Chinese state's alleged cyberattacks as not out of keeping with global norms. Around half of Qin's remarks accused the U.S. government of conducting cyberattacks and denounced the U.S.'s conduct: "US government and relevant US institutions have long been involved in large-scale and organized cyber theft" (Qin 2014). Purporting to speak in defense of the social norms of the international community, Qin further asserted that the U.S.'s global status was under threat and sought to establish China's innocence: "The US acts are receiving wide- spread condemnation from all

countries and the world opinion. China is a victim of severe US cyber theft, wiretapping and surveillance activities" (Qin 2014).

What was Qin attempting to accomplish by accusing the U.S. of cyberattacks? I argue that Qin's statement was trying to establish that if the Chinese government's alleged cyberattacks were 'criminal,' then the U.S. government was just as culpable. Recall that criminality is socially constructed; actions that constitute crimes are not inherently 'criminal,' but rather, are *deemed* unacceptable misconduct from the perspective of a given society. If everybody in society is committing actions that constitute 'crimes,' then those actions arguably become the norm, ergo they are not 'crimes.' By accusing the U.S. government of having engaged in the same type of cyberattacking conduct alleged in the indictment, the Chinese state seemed to be wagering that the U.S. would never accept that both the U.S. and China were two 'criminal outcasts,' and that the U.S. and other members of the international community might instead concede that the U.S. and China were both in the right. The Chinese state was attempting to establish its innocence not through providing evidence to directly refute the U.S.'s accusation that the Chinese state had engaged in these cyberattacks, but rather, by justifying the alleged cyberattacks as not having been out of keeping with international norms – in short, by disputing that China's alleged actions were *criminal*.

Overall, Qin's statement suggests that the Chinese state's priority was not to directly refute the accusation that it had perpetrated the actions alleged in the indictment. Rather, China's focus was on arguing that its alleged actions were not out of keeping with global norms, and that these actions would therefore not constitute misconduct among the international community. The Chinese state did not directly refute its officers' perpetration

of the cyberattacks themselves, but rather, sought to reposition these alleged cyberattacks as not constituting misconduct. This analysis of Qin's statements evidences the contention that China was responding to the *criminal* nature of the naming-and-shaming achieved by the bare indictment's public attack to China's national face. Qin's statement centered on arguing that China's alleged cyberattacks would not be considered 'crimes' in the international society.

In addition to portraying the U.S. accusation of criminality as being inconsistent with international norms, Qin further criticized the U.S.'s actions as diplomatically unsound with respect to foreign relations, saying that the indictment "jeopardizes U.S.-China cooperation and mutual trust" (Qin 2014). One year later, however, a cooperative milestone on cybersecurity matters was reached by the respective heads of state of the two nations. In September 2015, U.S. President Barack Obama and Chinese President Xi Jinping arrived at an agreement that was committed to writing by and immediately released via the U.S. White House's Office of the Press Secretary (White House 2015). Interestingly, and in contrast to Qin's dire prediction of undermined relations between the U.S. and China, the written text of Obama's and Xi's September 2015 agreement expressly invoked cooperation. The first of four provisions on cybersecurity reads in part, "both sides agree to cooperate… with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory" (White House 2015). The second, which has been the focus of much analysis and debate (Harold 2016; Farley 2018; Lin 2018), constrained each party's own conduct not only toward the other nation, but toward the entire world. Under the second provision of the agreement, neither the U.S. nor China would condone hacking if the purpose were to steal information to be used for

private profit, irrespective of the target of such hacking: "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" (White House 2015). The agreement also addressed international norms, as the third of the cybersecurity provisions begins, "Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community" (White House 2015).

It seems, then, that this "Cyber Agreement" between Xi and Obama resolved at least part of the question on what type of conduct would be considered 'misconduct' with reference to the social norms of the global community. However, my reading of the agreement's overly narrow scope yields an argument that any deterrent effect accomplished by this agreement would be very limited. Pursuant to the terms of the agreement, both the U.S. government and the Chinese government would consider a narrow subset of cyberattacks to be misconduct if the cyberattacks in question met three criteria. One was that the cyberattack must be unauthorized access that leads to a taking of data; this type of cyberattack can be contrasted with – for instance – a DDoS attack, which does not take data. Two, the taking must be of "intellectual property," as opposed to a cyberattack that takes – for example – credit card numbers. Three, it would have to be established that the cyberattacks' purpose was to "[provide] competitive advantages to companies or commercial sectors" (White House 2015). Besides the arguable difficulty in practice of establishing this purpose, the narrowness of this third criterion leaves open myriad possibilities for any cyberattack involving unauthorized access to be exempt from

being considered misconduct under the terms of this agreement, so long as it can be argued that any data being taken is being used for some purpose other than "providing competitive advantages to companies or commercial sectors" (White House 2015). Arguably, the definition of misconduct is overly narrow. This analysis of the agreement suggests that any deterrent norm-setting accomplished by the 2015 cyber agreement would be extremely limited in scope; I would therefore argue that the Cyber Agreement achieved very little, if any, general deterrent effect.

Furthermore, I would call attention to another practical shortcoming: it is unclear how and to what extent this agreement could be enforceable. That is to say, even if one of the governments decided to overtly breach this provision of the agreement, such that it could be easily proven that the cyberattacks in question met the three criteria for the definition of misconduct, what recourse would the other party have to make that government comply with the agreement? In light of the overly narrow scope of the norm-setting, the difficulty in praxis of proving intent, and the limited enforceability of the agreement, this provision lacks deterrent force.

Indeed, scholars have debated the efficacy of the Xi-Obama cyber agreement and whether it contributed at all to constraining the conduct of the Chinese state (Harold 2016; Goldsmith 2016; Goldsmith and Williams 2018; Farley 2018; Lin 2018). I suggest, however, that the salience of the Cyber Agreement as a remarkable about-face from Qin's dire predictions and an arguable watershed moment in U.S.-China diplomatic relations distracts from another event that my analysis argues is likely responsible for deterrence. It was the deterrent effects of the unilateral U.S. bare indictment in May 2014, rather than

any deterrent effects of the bilateral U.S.-China cyber agreement in September 2015, that prompted a dramatic decline in Chinese cyberattacks.

4.2.3. The Timing of the Steep Decline in Chinese Cyberattacks Coincides with the May 2014 Bare Indictment

Has a deterrent effect been achieved against cyberattacks originating from China? This question has been the subject of much scholarly debate; I contend that looking to the data on hostile cyber operations technically attributed to the Chinese state shows that the answer is yes. Technology reporters such as Ellen Nakashima of the *Washington Post* and Andy Greenberg of *Wired* have pointed to evidence of a deterrent effect: in the months following the indictment, China's cyberattacking activity against commercial targets dramatically declined. In a piece for the *Washington Post* on November 30, 2015, shortly after the September 2015 U.S.-China cyber agreement between Xi and Obama, Nakashima wrote that "current and former U.S. officials" suggested that intelligence indicated that "The Chinese military scaled back its cybertheft of U.S. commercial secrets" immediately after the bare indictment (Nakashima, November 30, 2015). Writing on December 16, 2016, Greenberg observed, "the last year has seen a little-discussed but dramatic *drop* [italics in original] in Chinese state-sponsored hacking, particularly for intrusions targeting private companies" (Greenberg 2016). While Nakashima's November 2015 piece had cited to U.S. officials with knowledge of the situation, Greenberg's December 2016 article was able to cite to a technical attribution report that was prepared by the private cybersecurity firm Mandiant and publicly released in June 2016.

Surprisingly, however, this June 2016 Mandiant report was hesitant to interpret the data as evidence of a deterrent effect: "Rather than viewing the Xi-Obama agreement as a watershed moment, we conclude that the agreement was one point amongst dramatic changes that had been taking place for years" (Mandiant 2016, 15). Jack Goldsmith, who has authored and co-authored critical pieces questioning the effectiveness of the U.S. government's strategic use of bare indictments as a deterrent measure against cyberattacks, analyzed the same Mandiant report in a piece for *Lawfare* on June 21, 2016; observing that "The report shows that most of the drop-off in China-based cybertheft occurred before the Obama-Xi agreement last Fall," Goldsmith argued that the decline was due to an internal anti-corruption campaign that Xi instituted in 2013 (Goldsmith 2016). Goldsmith argued this point more forcefully in a 2018 piece co-authored with Robert D. Williams and entitled "The Failure of the United States' Chinese-Hacking Indictment Strategy." Acknowledging that some U.S. officials and analysts had indicated that the 2014 bare indictment against the PLA Unit 61398 officers was used by the U.S. as a diplomatic pressure point to prompt the 2015 Xi-Obama cyber agreement (Nakashima 2015, Harold 2016), Goldsmith and Williams argued that "deterrence-by-indictment efforts have failed" and that measurement issues or the anti-corruption campaign were responsible for the seeming decline: "It is now better understood that the apparent slowdown in China's cybertheft after the [2015][13] agreement was more likely due to two factors: (1) China's hackers grew more operationally sophisticated and began to hide their tracks (or their connections to state entities) better; and (2) Xi's centralization reforms and anti-corruption

[13] The original text from Goldsmith and Williams reads "2014," which is likely a typographical error since earlier passages in this Goldsmith and Williams article refer to the date of the Xi-Obama agreement as 2015.

campaign cracked down on unauthorized cybertheft freelancing" (Goldsmith and Williams 2018).

Detection issues – the first of Goldsmith's and Williams' two factors – can be rebutted because Mandiant's 2016 technical attribution results showing a decline in Chinese cyberattacking activity have been validated by other private cybersecurity firms. For example, Greenberg's 2016 piece quoted the chief technology officer ("CTO") from the private cybersecurity firm Crowdstrike. Affirming the results of the 2016 Mandiant report, Crowdstrike's CTO stated that "his company… has seen a similar falloff in Chinese hacking incidents" (Greenberg 2016). The CTO also anticipated and rebutted the counterargument that "the attacks have only become more sophisticated, and harder to detect" (Greenberg 2016). If technological advancements in Chinese cyberattacking methods and tactics were responsible for the observed decline, then the expectation would be that there would be few or no observations of older methods and tactics. By contrast, Crowdstrike had observed that the older methods and tactics were still actively employed in the cyberattacks that continued to be technically attributable to the Chinese state: "the same methods seen previously are still used against some high-value government targets" (Greenberg 2016). That is to say, among the few observable cyberattacks that continued to be mounted from China, the same techniques were still in use. If Chinese cyberattackers had developed new, undetectable techniques and had shifted to using these new undetectable techniques, the expectation would be that the new techniques would replace the old techniques, so there would be few or no observations of the old techniques in use. However, Crowdstrike instead recorded many instances of the old techniques in use among the observable Chinese cyberattacks. The assumption is that for its most ambitious

cyberattacks against "high-value government targets," Chinese cyberattackers would use the most advanced techniques available to them. By contrast, the evidence shows that as of December 2016, Chinese cyberattackers were still deploying the old techniques against these "high-value targets"; this evidence suggests that there were not new, undetectable techniques available to Chinese cyberattackers at that time. It is possible that the deployment of old techniques to obfuscate the deployment of new techniques could be a deliberate, strategic misdirect by Chinese cyberattackers, but this seems unlikely. Marshalling a detectable cyberattack when an undetectable one was available would consume valuable resources such as computing power, as well as the human cyberattacker's attention and effort. Moreover, research has not yielded evidence to suggest a deliberate misdirect. Therefore, it is unlikely that the observed drop in Chinese cyberattacks is due to issues with detecting advanced techniques.

As for the second factor, I suggest that critics' data interpretations – in a reversal of the popular idiom – have missed the trees for the forest. By focusing on large-scale trends in Chinese cyberattacking activity against commercial targets, these interpretations lose sight of smaller-scale details regarding when the trend started.

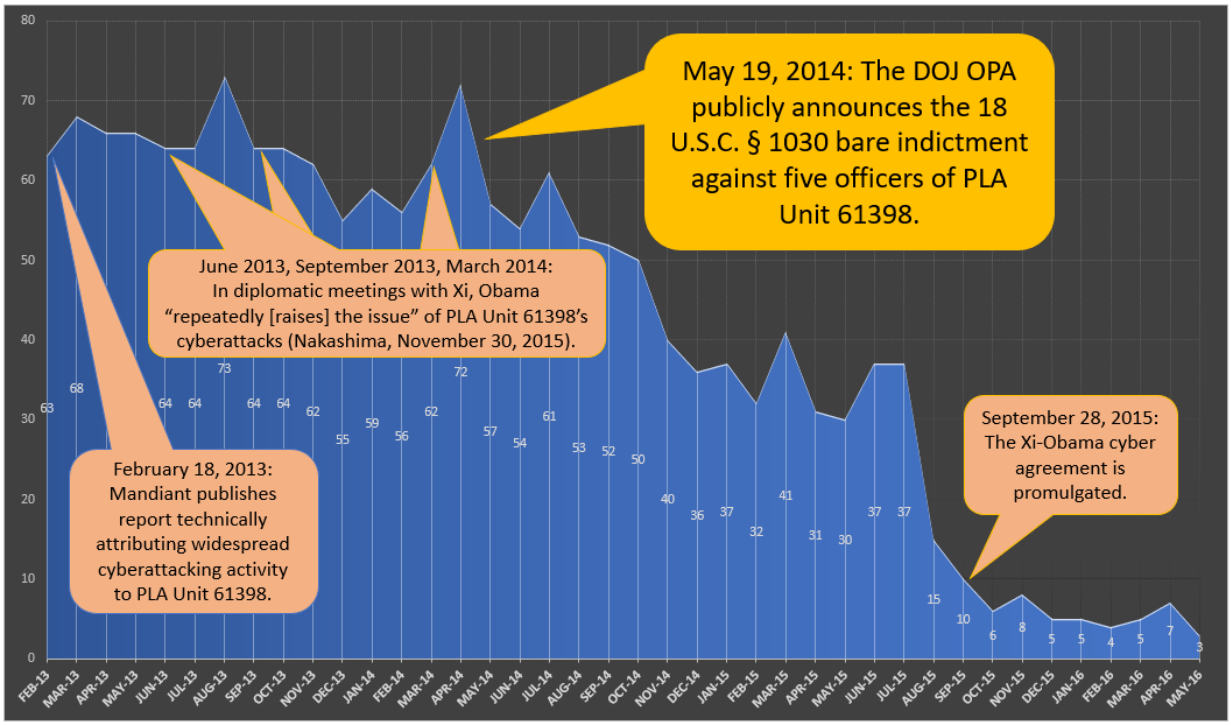
In the months preceding May 2014, the cyberattacking activity that Mandiant found technically attributable to the Chinese state was on the rise. This upward trend started in December 2013, with 55 "active network compromises by suspected China-based groups" recorded by Mandiant. This number rose to 59 in January 2014; after a small drop to 56 in February 2014, the number was around 62 in March 2014 and reached a high of 72 in April 2014. After this recorded rise in Chinese cyberattacking activity, the number dropped

down to 57 in May 2014 and even further, to 54, in June 2014. As scholars and analysts have recognized, Mandiant's data show that recorded Chinese cyberattacking activity overall precipitously declined from May 2014 to May 2016, since the number dropped from 72 to 3. In contrast, as Goldsmith and others have noted, the number was already low – at 10 – when the 2015 cyber agreement between Xi and Obama was promulgated.

In the following Figure I, the x-axis on the graph represents date by month, ranging from February 2013 to May 2016; the y-axis represents the number of cyberattacks that Mandiant observed and technically attributed to Chinese cyberattackers. This data on the number of Chinese cyberattacks is adapted from Mandiant's chart "Active Network Compromises Conducted by 72 Suspected China-Based Groups by Month" (Mandiant 2016, 11). Text box callouts indicate possible events that could have deterred cyberattacks originating from China. One of these events is the aforementioned September 2015 promulgation of the Xi-Obama cyber agreement. Two more of these events, which will be further discussed in Section 4.2.4., are Mandiant's February 2013 publication of a technical attribution report naming PLA Unit 61398; and Obama's diplomatic meetings with Xi between June 2013 and March 2014, in which Obama iteratively problematized the cyberattacks that Mandiant had technically attributed to PLA Unit 61398. This graph shows that other events that could arguably have achieved a deterrent effect are not temporally associated with any recorded drastic decreases in Chinese cyberattacking activity. Indeed, the graph shows that the number of active cyber intrusions that Mandiant technically attributed to Chinese cyberattackers either remained static or weakly rose for the respective month that followed each of these other events. The graph shows, by contrast, that the interruption of a rising trend in Chinese cyberattacking activity – and the

change to a large-scale trend of decline – exactly coincides with the May 2014 publicization of the bare indictment against the five members of PLA Unit 61398.

FIGURE I. POSSIBLE DETERRENT EVENTS PROMPTING THE STEEP DECLINE IN CYBERATTACKS ORIGINATING FROM CHINA, FEB. 2013 TO MAY 2016



It could be argued that this evidence on the timing of the change from a rising trend to a declining trend is not necessarily dispositive of the argument that Xi's internal anti-corruption campaign was responsible for the decline. However, in light of the sheer amount of cyberattacking activity that was technically attributed to the Chinese government, and the fact that much of the taken data aligns with what the Chinese state considers markers of national prestige, it seems implausible that the widespread campaign

of cyberattacking behavior technically attributed to Chinese state-sponsored actors such as PLA Unit 61398 was the work of rogue, corrupt officials that the Chinese government disapproved of yet was unable to bring under control. Qin's public statement, for instance, did not condemn the alleged cyberattacking activity as the work of rogue agents; the Chinese government's official response did not focus on problematizing the alleged cyberattacking behavior itself, but rather, concentrated on disputing the criminality of this behavior.

Moreover, an explanation that China ignored the U.S. bare indictment, that Xi's early 2013 anti-corruption campaign lay dormant for a year and a half, and that Xi's anti-corruption campaign had always planned to crack down on rogue cyberattacking activity starting in May 2014 would involve far more than a remarkable coincidence. The indignant response immediately issued by the Chinese government spokesman shows that the bare indictment did not go unnoticed by the Chinese state; with this proof that the information on the bare indictment was successfully communicated to and received by the Chinese government, it is likely that Chinese state-linked cyberattackers would have factored the consequence of bare indictment into their cost-benefit calculus.

Further reinforcing the deterrent effect is the evidence that the bare indictment was not only communicated to China, but also that China contemplated the bare indictment as a deterrent threat: the Chinese state spokesman's response aligns with the predictions of the theory, as the indignance in the May 20, 2014 public statement indicates that China saw the bare indictment as an attack on status. Despite the 2013 institution of Xi's anti-corruption campaign, recorded Chinese cyberattacking activity was on the rise in the months

immediately preceding the May 2014 public announcement of the bare indictment's unsealing; the about-face to a declining trend occurred in exactly the month that the bare indictment was issued.

Thus, the null hypothesis that the bare indictment did *not* achieve a deterrent effect, as well as the counterargument that other factors such as an anti-corruption campaign were responsible for the dramatic decline in Chinese cyberattacking activity, are not as well supported by the data. Proof of the bare indictment's deterrent effect might be made even stronger if more fine-grained data, recording China's cyberattacking activity during the month of May 2014 day-by-day, were made available. The expectation is that such data would show that the decline in Chinese cyberattacking activity began not before May 19, 2014, but rather, in the days following the U.S.'s May 19, 2014 public announcement of the bare indictment's unsealing.

4.2.4. Criminal Naming-and-Shaming versus Other Explanations

With it having been shown that the bare indictment did deter the Chinese state from committing further recidivist cyberattacks, the next question to be addressed regards what aspect of the bare indictment achieved the deterrent effect. As discussed in Chapter 3, this theory contends that the package of informal sanctions triggered by the label of "criminal outcast" served to frustrate the Chinese state's prestige-seeking objectives in mounting cyberattacks targeting scientific and business information. The public announcement of the bare indictment's unsealing enabled other potential offenders within the Chinese state to factor these negative consequences, most importantly denial of status, into their cost-

benefit calculus. Since the features of a bare indictment mean that it can convincingly label indicted actors "criminal outcasts," the bare indictment achieved a general deterrent effect by lowering the potential offenders' expected benefit of status. Bare indictments' attack to face can achieve deterrent effects because the attack to face consists of public criminal naming-and-shaming. Neither mere publicization of technical attribution results nor non-criminal naming-and-shaming can achieve the same deterrent effects; the combination of these components makes bare indictments a unique policy instrument.

My theoretical contentions, then, can be further supported by disproving competing contentions. Scholars who contend that bare indictments do have a deterrent effect have also seen bare indictments as an attack on the Chinese state's status, but these scholars locate the mechanism in other constituent functions of bare indictments rather than in the combined features of what makes a bare indictment an effective attack on face. Scholars have suggested two functions of bare indictments – the technical attribution function and the "name-and-shame" function – that may be responsible for effecting deterrence. For clarity, I will refer to this second function as the *civil* naming-and-shaming function, as opposed to the *criminal* naming-and-shaming that I argue makes up part of the informal sanctions of bare indictments. The technical attribution function and the civil name-and-shame function may overlap in that technical attribution forms the foundation for civil name-and-shame, but legal scholars have discussed them as distinct concepts (Keitner 2019; Hinck and Maurer 2019). The technical attribution function of bare indictments regards publicly announcing the results of technical attribution. Garrett Hinck and Tim Maurer present this function as the most salient, "primary purpose of unsealing criminal charges" (531, 2020). Likewise, Chimène Keitner's article "Attribution by Indictment"

suggests that bare indictments' technical attribution function in making the results of technical attribution publicly known may be responsible for a deterrent effect, because the execution of this function eliminates doubt that U.S. parties are able to technically attribute cyberattacks: "Detailed cyber-related indictments demonstrate U.S. capabilities for detecting and identifying malicious cyber activity" (Keitner 2019, 211). While Hinck and Maurer (2019) identify the technical attribution function as the most salient feature of bare indictments, a 2020 article by those authors is skeptical that the technical attribution function can achieve deterrence, saying "by itself attribution is not a deterrence strategy" (2020, 533); technical attribution alone does not raise cyber adversaries' expected costs such that the adversaries will be deterred.

Pointing to another function that could be responsible for achieving a deterrent effect, Hinck and Maurer discuss the civil name-and-shame function: "labeling certain behavior as deviant" may raise the expected costs of the perpetrators of that behavior (Hinck and Maurer 2020, 533). John Carlin, who in his role as U.S. Assistant Attorney General for National Security actively shaped the U.S.'s cyber indictment strategy (Viswanatha and Mann 2015), has repeatedly positioned the civil name-and-shame function as the purpose of the U.S.'s cyber deterrence strategy (Carlin 2016; Viswanatha and Mann 2015; Tucker and Abdollah 2016; Lucas 2019). By contrast, Goldsmith (2020) continues to be critical of the effectiveness of the civil name-and-shame function and technical attribution function. According to Goldsmith, demonstrating the U.S.'s technical attribution capability does not reveal to cyber adversaries any new information that could have a deterrent effect, and "naming and shaming is not much accountability" (2020).

Although Goldsmith's work – as discussed above – is skeptical that bare indictments achieve a deterrent effect at any appreciable level, the PLA Unit 61398 case study provides evidence for his arguments that it is neither the technical attribution function nor the civil name-and-shame function of bare indictments that is dispositive in causing a deterrent effect. Preceding the unsealing of the bare indictment in the PLA Unit 61398 case, other strategic moves originating from the U.S. carried out, respectively, the technical attribution function and the civil name-and-shame function. Nonetheless, unlike the bare indictment against the five PLA Unit 61398 officers, these moves did not seem to deter the Chinese state. Nakashima (July 09, 2015) points to an earlier technical attribution report that was prepared and publicly released by Mandiant in February 2013. The 2013 Mandiant report carried out the technical attribution function by publicly announcing its capabilities to technically attribute cyberattacks – cyberattacks similar to the ones later described in the indictment – to PLA Unit 61398. The 2013 Mandiant report even went so far as to technically attribute the cyberattacks to individual PLA Unit 61398 officers, such as Wang Dong, who was later the lead defendant charged by the May 2014 bare indictment (Mandiant 2013, 52-55).

As the 2013 Mandiant report went into great detail to demonstrate the integrity of its technical attribution methodology, it could be argued that the 2013 Mandiant report executed the technical attribution function even more effectively than the 2014 bare indictment later would – yet the 2013 Mandiant report failed to achieve a deterrent result. In April 2013, a representative of Mandiant acknowledged that there had been "no change" in Chinese cyberattacks against U.S. commercial firms (Wall Street Journal 2013). If anything, the 2013 Mandiant report may have provoked more cyberattacks by the Chinese

state; in a seeming attempt to besmirch the credibility of the 2013 Mandiant report, hostile cyberattackers soon embedded malware into the digital file of the 2013 Mandiant report (Finkle 2013), using the report as a delivery vehicle for gaining unauthorized access or damaging computer systems.

According to Goldsmith, the 2013 Mandiant technical attribution report and the May 2014 bare indictment coincided in their substantive content (Goldsmith 2014). I would therefore point out that the May 2014 bare indictment accomplished very little that was 'new' where publicizing technical attribution results was concerned, since publicization of technical attribution results had already been done by Mandiant in February 2013. Yet, the data indicate that the deterrent result coincides with the May 2014 bare indictment, not Mandiant's February 2013 technical attribution report. Since both the February 2013 Mandiant report and the May 2014 bare indictment carried out the technical attribution function but only the May 2014 bare indictment was closely followed by a decline in Chinese cyberattacks, the technical attribution function could not have been responsible for causing this deterrent result.

Likewise, there is evidence that indicates that the civil name-and-shame function was iteratively executed in the U.S.'s diplomatic communications with China. Nakashima writes that the 2013 Mandiant report "freed the administration to speak more openly about the Chinese cyber-campaign, as officials could point to the document to buttress their assertions. Obama repeatedly raised the issue with Xi — in Sunnylands, Calif., in June 2013; in St. Petersburg, Russia, in September of that year; and again in The Hague in March 2014" (July 09, 2015). Even though Obama positioned the Chinese state's alleged cyberattacks as

problematic behavior and named the Chinese state as the perpetrator of that behavior, this iterative naming-and-shaming did not seem to have an appreciable deterrent effect on Chinese cyberattacking activity. Mandiant's chart, reproduced in annotated form above, shows that Chinese cyberattacking activity remained at much the same level between February 2013 and March 2014, with no month-to-month drop of the scale recorded for the period between April 2014 and May 2014 (Mandiant 2016, 11).

With these competing explanations of the technical attribution function and the civil name-and-shame function ruled out, I suggest that these functions – while not dispositive of the decline – may capture part of the causal mechanism at play. The shaming effect of Obama's diplomatic discussions with Xi are comparable to that which would have been achieved by accusing the Chinese state of an offense under civil law. As mentioned in Chapter 2, a civil wrong is often traceable to a disagreement between two or more private parties, whereas a criminal wrong can be conceptualized as an unacceptable offense against society. Shaming an adversary by accusing them of a civil wrong is like saying that the adversary 'does not work well with others,' but denouncing an adversary as uncooperative, disagreeable, or unprofessional is less severe of an insult than shaming an adversary by labeling them a "criminal" who has committed an offense against society as a whole. As scholars have theorized, technical attribution laid the groundwork for the execution of the name-and-shame function, but it was not shaming via labeling the Chinese state's cyberattacks as merely "deviant" that achieved the deterrent effect. Rather, it was shaming via labeling the Chinese state's cyberattacks as *criminal*, the worst type of social deviance; being labeled a criminal outcast is far more inconsistent with holding a prestigious position in the status hierarchy than is being labeled someone who behaves in

an aggressive or disagreeable manner. Criminal naming-and-shaming via a public attack on status is, here, one component of the package of informal sanctions that is triggered by the label of "criminal outcast"; it is this part of the package that, in the PLA Unit 61398 case, deterred the Chinese state by denying its prestige-seeking aims.

In sum, looking to the timing of the steep decline in Chinese cyberattacks and ruling out alternative explanations for the sudden drop have shown that the issuance and publicization of the bare indictment in the PLA Unit 61398 case achieved deterrent effects against the Chinese state. This can be conceptualized both as general deterrence of potential Chinese cyberattackers, and as specific deterrence against the Chinese state itself.

4.3. Profit-Seeking Lazarus Group Undeterred in Illicitly Raising Revenue for North Korea [NK-01]

On February 17, 2021, the unsealing of a federal indictment against three North Korean nationals was announced by the DOJ's OPA. The indictment alleged that these three individuals were employed by the Reconnaissance General Bureau ("RGB"), a "military intelligence agency" of North Korea, to carry out cyberattacks on behalf of the North Korean state; RGB's cyberattackers are known in cybersecurity circles as the "Lazarus Group" (Dugas 2022). As the indictment alleged, these three Lazarus-affiliated individuals had taken at least hundreds of millions in U.S. dollars ("USD") from mounting several cyberattack-enabled virtual heists from cryptocurrency exchanges and financial institutions worldwide (*U.S. v. Jon* indictment).

I analyze these state-sponsored heists in the context of North Korea's policy objectives to show why, as predicted by the theory, the bare indictment could not achieve a specific deterrent effect against the Lazarus Group: the package of informal sanctions triggered by bare indictment could neither directly counteract nor indirectly outweigh the Lazarus Group's profit-seeking motive of illicitly raising revenue for the North Korean state. First, I present analysts' and officials' consensus that, in light of the Lazarus Group's connections to the North Korean government and the North Korean government's revenue-raising objectives, the Lazarus Group's cyberattacks are primarily motivated by profit-seeking. Then, I provide an overview of the case to show evidence that the cyberattackers are obviously undeterred.

Scholars, practitioners, and other analysts who have endeavored to determine why the state-sponsored Lazarus Group mounts its cyberattacks are generally in agreement that the Lazarus Group's aim is illicitly raising revenue for North Korea. In a 2017 piece for *Wired* on "[understanding] the motivations of the Hermit Kingdom's hackers," technology reporter Andy Greenberg starts by looking to the characteristics of the cyberattacks, describing them as "outright theft" (Greenberg 2017). Quoting three security researchers and a foreign policy scholar, Greenberg (2017) presents profit-seeking as the motivation for the crime, given the North Korean state's need for monetary resources:

> The motive makes sense: North Korea needs the money. As a result of its human rights abuses, nuclear brinksmanship, and sociopathic aggression toward its neighbors, the country faces crippling trade sanctions. Before its hacking spree, it had already resorted to selling weapons to other rogue nations, and even run its own human trafficking and methamphetamine production operations. Cybercrime represents just another lucrative income stream for a shameless, impoverished government.

Likewise, cybersecurity law analyst Mari Dugas, writing in *Just Security* two weeks after the indictment's unsealing, calls attention to how these three individuals' cyberattack-enabled heists make a substantial contribution to the North Korean state's revenue: "The indictment shows just how consequential North Korea's cyber operations are to its gross domestic product (GDP), with the hackers obtaining a total $1.3 billion from their different attacks… For a country with an estimated GDP of only $28 billion, this is an enormous sum of money obtained from hacking" (Dugas 2021). Dugas also cites an article from *Reuters*, which states that a 2019 United Nations report estimated North Korean state-sponsored hackers' takings to have been "up to two billion US dollars" (Nichols 2019).

Even a more conservative estimate generated by an alternative method of summing the monetary value of the three cyberattackers' takings proves the point. Dugas' $1.3 billion USD figure is described in the indictment as the value of the funds that the three individuals "*attempted* to steal or extort [emphasis added]" (*U.S. v. Jon* indictment, 2). Adding the monetary values that the indictment describes as having been *successfully* taken by the three individuals yields a total of over 872.5 million USD in monetary funds. The earliest monetary taking listed by the indictment occurred in December 2015, and the latest monetary taking occurred in August 2020. The Bank of Korea estimated North Korea's 2020 gross domestic product to be 27.4 billion USD (Jones 2021). As a proportion, the total that the indictment lists as successfully having been taken by the three defendants is over three percent of the Bank of Korea's estimate. From this information, it can be calculated that three individuals were allegedly responsible for conspiring to successfully take – in a span of under five years – monetary funds totaling to an amount over three percent of the North Korean state's 2020 estimated gross domestic product.

U.S. government officials also recognize and characterize North Korea's cyberattack-enabled heists as profit-seeking. Announcing the earlier unsealing of criminal charges against one of the three individuals, U.S. Secretary of the Treasury Steven Mnuchin stated in September 2018 that North Korean state-sponsored cyberattackers' objective was to "generate illicit revenues" (DOJ OPA, September 06, 2018). Likewise, in a public statement in connection with the DOJ's August 2020 civil forfeiture suit to recover the monetary funds that had allegedly been taken by North Korean state-sponsored actors, Brigadier General Joe Hartman – whose title was stated to be Commander of the Cyber National Mission Force – implicitly characterized the cyberattack-enabled heists as profit-seeking. Hartman stated that the overarching goal of the U.S.'s civil forfeiture suit was "disrupting North Korean attempts to illicitly generate revenue" (U.S. Attorney's Office, District of Columbia, August 27, 2020).

Resonating with Hartman's statement that the priority is to disrupt rather than to deter, the primarily profit-seeking motivation of the cyberattack-enabled heists allegedly perpetrated by these North Korean state-sponsored actors leads to the theoretical prediction that the bare indictment would not deter the actors from committing recidivist cyberattacks. Labeling the alleged offenders "criminal outcasts" may deter prestige-seeking actors by lowering their expected benefit, but an attack on prestige is not a direct frustration of the profit-seeking motive. The package of informal sanctions can, by increasing the potential offenders' expected cost, outweigh thrill-seeking motivations; however, it is not enough to outweigh the expected benefit of garnering amounts equal to a substantial portion of the country's gross domestic product.

As predicted, evidence indicates that the Lazarus Group was obviously undeterred by the 2021 unsealing of the bare indictment. *Wired* reports that two private cybersecurity firms conducting technical attribution on a cyberattack-enabled heist perpetrated in March 2022 have named the perpetrator as the Lazarus Group (Newman 2022). The monetary value of the amount successfully taken from the cryptocurrency exchange by the Lazarus Group is estimated to be more than 600 million USD (Newman 2022). The U.S. government continues to devote attention to disrupting the Lazarus Group's operations through economic sanctions, which indicates that the U.S. government regards the Lazarus Group as an active threat.[14]

4.4.0. Bare Indictments Outweigh The Thrill of Cyberattacks [IRAN-06]

On November 28, 2018, the DOJ's OPA publicly announced the unsealing of an indictment that had been filed two days prior against two Iranian nationals. The indictment alleged that the two individuals had violated 18 U.S.C. § 1030 by using "SamSam Ransomware," malicious software ("malware") that the two individuals created, to gain unauthorized access to the computer systems of victims such as hospitals and municipal governments; the malware would then hold the victims' sensitive data hostage by rendering it inaccessible to authorized users unless a monetary ransom were paid to the two individuals (*Savandi* indictment). The Federal Bureau of Investigation ("FBI") issued

[14] Although this *Wired* article describes the U.S. Treasury's actions as the imposition of "expanded sanctions" (Newman 2022), this terminology is slightly misleading; it is not the scope of the economic sanctions against the Lazarus group that was expanded. Rather, the Lazarus Group's listing on the Specially Designated Nationals and Blocked Persons List ("SDN List") was updated with three more digital currency addresses by which the Lazarus Group could be identified. Such updates, adding more digital currency addresses to the Lazarus Group's listing on the SDN List, have been made as recently as May 06, 2022 (U.S. Department of the Treasury, May 06, 2022).

its own press release, which portrayed the indictment as a bare indictment since it stated that FBI intelligence knew the two individuals to be physically located in Iran and "currently out of the reach of U.S. law enforcement" (FBI, November 28, 2018). Despite these apparent limitations, SamSam Ransomware has not been deployed since the bare indictment's unsealing in November 2018.

In this section, I look to chronology to argue that the bare indictment was responsible for deterring the two accused cyberattackers from perpetrating further cyberattacks because the indicted individuals were primarily motivated by thrill-seeking, a motive that was outweighed by the emotional and practical consequences in the package of informal sanctions that is triggered by bare indictments. Thus, I use the SamSam Ransomware case study as an example to demonstrate that bare indictments can deter thrill-seeking actors by outweighing the benefit of emotional thrill.

This section proceeds as follows. First, I outline the chronology of the case to show that it was the bare indictment – not other events that could arguably have served the same function as some constituent components of the bare indictment – that put an abrupt end to the campaign of criminal activities perpetrated by the creators of SamSam Ransomware. Then, I show that while the actors' motive in mounting this ransomware scheme may initially seem to be profit-seeking, an examination of the information in the indictment and the surrounding circumstances supports an argument that the cyberattackers were, instead, primarily motivated by thrill-seeking. The determination of the SamSam cyberattacks' thrill-seeking motives predicts that, and hence explains why, the SamSam cyberattacks would come to an immediate halt after the publicization of a bare indictment naming the alleged perpetrators of the cyberattacks.

4.4.1. Following Publicization of Bare Indictment, Cyberattacks Immediately Halt

As shown by the stamp of the clerk of court, the indictment charging Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri with violations of 18 U.S.C. 1030 was filed on November 26, 2018 (*Savandi* indictment). The indictment's unsealing was publicly announced two days later, on November 28, 2018. The indictment alleged that Savandi and Mansouri, both Iranian nationals, had "engaged in an international computer hacking and extortion scheme" beginning in December 2015 and continuing to the present date of the indictment (*Savandi* indictment). The indictment identified Savandi and Mansouri as the creators of SamSam Ransomware and accused them of having used the malware to gain unauthorized access to the computer systems of over two hundred victims whose data was then held hostage and rendered inaccessible to its authorized users unless the victim were to pay a monetary ransom in Bitcoin, a type of virtual currency (*Savandi* indictment). The indictment estimated that the ransom payments totaled over six million USD; furthermore, the damage caused to the victims' computer systems was estimated at over thirty million USD (*Savandi* indictment).

Prior to the indictment's issuing, SamSam Ransomware had drawn attention for its deployers' seeming mercilessness in choice of targets. In a research report released publicly on July 19, 2018, the private cybersecurity firm Sophos stated, "SamSam has made headline news for its attacks on organizations in the Healthcare, Government and Education sectors" (11). Although Sophos' report did not name Savandi and Mansouri, its findings on technical attribution pointed to clues that suggested that SamSam Ransomware had been created and deployed by an individual operating in the Eastern Hemisphere

(2018, 18-20). The Sophos report also made many recommendations advising information technology professionals and decisionmakers of how to harden their institutions' cybersecurity defenses against a SamSam Ransomware attack (2018, 22-24).

Given the high-profile nature and merciless character of the SamSam Ransomware attacks, many expressed pessimism as to whether the indictment – especially since it was clearly a "bare" indictment – against SamSam Ransomware's accused creators and deployers would do anything to deter or otherwise prevent the attacks. The FBI's own press statement seemed to frame the indictment as lacking deterrent force, stating that the indicted individuals were known by FBI intelligence to be physically located in Iran and "currently out of the reach of U.S. law enforcement" (FBI, November 28, 2018). Writing for *Wired* in a piece published the same day as the DOJ's press release that publicly announced the indictment's unsealing, cybersecurity reporter Brian Barrett covered the sympathy-inducing victims targeted by SamSam Ransomware, the technical sophistication of the malware, and the U.S.'s lack of extradition treaty with Iran as reasons for skepticism as to "whether the indictment eventually stops or even slows SamSam attacks" (Barrett, November 28, 2018). Barrett quoted a cybersecurity researcher who stated that the most recent SamSam Ransomware cyberattack had taken place only four days prior to the time of Barrett's writing (November 28, 2018).

Remarkably, and in contrast to dire predictions that the bare indictment could do nothing to deter the cyberattackers, the SamSam Ransomware cyberattacks appear to have completely stopped as of the time of the indictment's unsealing. Research yields no relevant results on the activities of Mansouri and Savandi since 2018, other than a 2021 bulletin from the Newark office of the FBI describing them as 'fugitives' and soliciting

information that could lead to the arrest of the two individuals (FBI Newark 2021). The availability of technical attribution tools means that it is highly unusual for there to be no reports on cyberattacks suspected to be perpetrated by known cyberattackers unless the cyberattackers have, in fact, ceased mounting cyberattacks. For example, Sophos' report described SamSam Ransomware as the focus of an ongoing research project; if SamSam Ransomware attacks had continued, Sophos or another private cybersecurity firm would likely have issued an updated report. In cybersecurity, such absence of evidence is itself extraordinary. Indeed, practitioners now consider SamSam Ransomware no longer active. Alina Georgiana Petcu, whose title is stated to be Product Marketing Manager for private cybersecurity firm Heimdal Security, writes, "mid to late 2018 seems to be the last year with publicly reported attacks linked to [SamSam Ransomware]… The [indictment] of the two Iranian hackers associated with the cybercrime operation seems to have been the terminus as far as incidents are concerned" (Petcu 2020).[15]

The chronology of the SamSam Ransomware case supports an argument that it was the bare indictment, not other events, that brought an abrupt end to the accused individuals' cyberattacks. The Sophos report could have deterred the SamSam Ransomware cyberattackers by raising their expected cost and lowering their expected probability of benefit. Showing vulnerable institutions how to harden their defenses would have made it more difficult for the cyberattackers to gain unauthorized access to potential victims' computer systems. Furthermore, Sophos' work in preventing SamSam

[15] The quote reads, "The **arrest** of the two Iranian hackers associated with the cybercrime operation seems to have been the terminus as far as incidents are concerned [emphasis added]" (Petcu 2020). This is likely a mistake. Petcu's memorandum is dated December 2020; as of the FBI's February 2021 bulletin, Savandi and Mansouri were described as still at large. Research yields no reports that Savandi and Mansouri have been arrested, and they remain listed on the FBI's Most Wanted as "SamSam Subjects." Based on this information, I have replaced Petcu's word "arrest" with the word "indictment."

Ransomware attacks could have had a deterrent effect because it was apparently known to the cyberattackers; in what could be perceived as a taunt by the cyberattackers, "On July 19, 2018 the main file in the SamSam ransomware was renamed to have a '.sophos' extension" (Sophos 2018, 7). As quoted by Barrett, SamSam Ransomware cyberattacks were taking place just four days before the indictment's unsealing. The grand jury proceedings that necessarily precede a federal criminal indictment would have been well underway four days before the indictment's unsealing, but since the existence of the grand jury hearing was not made known to the cyberattackers until the indictment was unsealed, the mere fact that grand jury proceedings were taking place could not have served as a deterrent. Although the Sophos report could have achieved a deterrent effect, the fact that SamSam Ransomware cyberattacks continued after the Sophos report's release and ceased abruptly after the public announcement of the bare indictment's unsealing indicates that the bare indictment was almost certainly responsible for deterring the accused perpetrators from committing further cyberattacks.

4.4.2. Determining Thrill-Seeking Motives of the SamSam Cyberattackers

Why did the bare indictment deter the SamSam Ransomware cyberattacks? The answer lies in the primarily thrill-seeking motives of the indicted cyberattackers. Recall that motive can be inferred from the behavior surrounding the perpetration of the crime; evidence on such behavior comes from the information in the indictment and from the surrounding circumstances of the case. If the cyberattackers were thrill-seeking, then this dissertation project's theory would predict that the package of informal sanctions triggered

by bare indictments would be likely to deter recidivist cyberattacks by outweighing the cyberattackers' expected benefit of emotional thrill.

With the charges stemming from a ransomware scheme that extorted monetary payments from victims, the contention that the SamSam Ransomware cyberattackers were primarily thrill-seeking rather than primarily profit-seeking may initially seem to ignore the obvious. However, the statistics in the Sophos report bear convincing indicia of thrill-seeking. For malware of this sophistication, the attackers could probably have gone after larger, wealthier targets and hence extorted much larger ransom payments. With this malware on their side, the cyberattackers might have extorted hundreds of thousands of dollars, rather than tens of thousands, per cyberattack. Although the cumulative total was around six million USD, it took cyberattacks on hundreds of victims to arrive at this total. Sophos' chart shows that the SamSam Ransomware cyberattackers' average ransom demand to each victim peaked at fifty-one thousand six hundred USD; average ransom demands were always in the tens of thousands and never approached the hundred-thousand-dollar mark, much less the million-dollar mark (Sophos 2018, 16).

If profit was the primary motive, then the attackers should have gone after wealthier targets who would have had the financial resources to fulfill much higher ransom demands yet might not have had the business infrastructure necessary to hold out on paying the ransom; an example of such a target is small businesses. SamSam Ransomware, as an advanced piece of malware, was certainly capable of gaining unauthorized access to more protected computer systems and holding hostage data of even greater value. Instead, the cyberattackers seemed to prey on victims in sectors that would elicit sympathy.

A counterargument would point to a data availability problem. Sophos' report surmises that SamSam Ransomware may have been used to attack private-sector businesses, and that the attacked private-sector businesses failed to report the cyberattacks (2018, 11-13). However, Sophos' report also states that *zero percent* of the hundreds of private-sector businesses that Sophos surmises were attacked by SamSam Ransomware reported the SamSam Ransomware attack as such (2018, 13). While private-sector businesses might have been loath to report such cyberattacks, it seems implausible that *no* private-sector businesses disclosed if SamSam Ransomware were used to target mostly private-sector businesses rather than mostly more sympathy-eliciting victims. Even the November 2018 indictment only mentions one private-sector business victim among eleven municipal, healthcare, or education victims (*Savandi* indictment, 2-3). Thus, it seems unlikely that data availability problems would call into question the contention that SamSam Ransomware was used to attack mostly sympathy-eliciting victims.

SamSam Ransomware was used to mount cyberattacks on a broad swathe of, it seems, as many sympathy-eliciting victims as possible. This may indicate that the perpetrators wanted to maximize their emotional thrill; if they had instead attempted to use SamSam Ransomware in perpetrating one lucrative cyberattack, they might have netted a higher payout, but they would only have had one thrilling experience instead of continually experiencing emotional thrills from conducting new cyberattacks over a period of three years.

Each ransom demand was relatively low, which does not comport with a primarily profit-seeking motive. Even a cumulative total of six million USD pales in comparison to the amount that could have been earned had SamSam Ramsomware's creators further

monetized their malware by offering it for sale to other cyberattackers. The lack of monetization means that profit-seeking is unlikely.

The taunts embedded in the cyberattacks' code are further indications of thrill-seeking. In addition to the possible taunt of Sophos mentioned above, SamSam Ransomware also bore embedded words of apology that could be construed as insincerely mocking the cyberattackers' victims (Sophos 2018, 11).

In statements made on November 28, 2018 and quoted in Barrett's piece, U.S. Attorney Craig Carpenito characterized the SamSam cyberattackers as a "new type of cybercriminal: money is not their sole objective" (Barrett, November 28, 2018). I have argued that money was not even the SamSam cyberattackers' primary objective; rather, the circumstances of the crime are consistent with a contention that Savandi and Mansouri were primarily motivated by thrill-seeking. The data on their targeting of a broad swathe of sympathy-eliciting victims, their choice of making low ransom demands when they could have easily deployed SamSam Ransomware to target victims capable of fulfilling much higher ransom demands, their decision not to monetize SamSam Ransomware to garner exponentially higher funds, and their taunting words toward Sophos and victims all point to this conclusion. Their primarily thrill-seeking motivation shows why they were deterred by bare indictment: thrill tends to be outweighed by informal sanctions. Despite that the FBI knows Savandi and Mansouri to be in Iran and out of reach of the imposition of formal legal consequences, it seems that the SamSam Ransomware cyberattackers were deterred by the imposition of informal sanctions. With the SamSam Ransomware cyberattacks having been technically attributed to Savandi and Mansouri, any one component of the package of informal sanctions triggered by their bare indictment could have deterred

Savandi and Mansouri. The chronology shows that bare indictments are likely the reason why the SamSam Ransomware cyberattackers completely ceased deploying SamSam Ransomware, and the reason why Savandi and Mansouri – the individuals to whom the SamSam Ransomware attacks were technically attributed – remain fugitives to this day.

4.5.0. Proof of Norm-Setting and General Deterrence: Chinese Cyberattackers' Shift from Status-Seeking to Profit-Seeking

In this section, I conduct a macro-level analysis of the next nine bare indictments accusing Chinese nationals of violating 18 U.S.C. § 1030; my analysis reveals a trend away from prestige-seeking motivations toward profit-seeking motivations. This section first very briefly revisits the theoretical underpinnings to show why such a trend would be indicative of the success of bare indictments as a deterrent measure and hence support the hypotheses on bare indictments' differing deterrent effects in accordance with cyberattacker motive. Then, I raise other scholars' competing explanations for this trend, which center on their interpretations of the 2015 Cyber Agreement between Xi and Obama. To show evidence of the predicted trend, I conduct brief case studies of each of the next nine 18 U.S.C. § 1030 bare indictments issued against Chinese nationals.

Recall the discussion in Section 3.4. If bare indictments tend to be an effective specific deterrent against status-seeking cyberattackers but tend not to specifically deter profit-seeking cyberattackers, the theory would predict that over time, a trend of more bare indictments against profit-seeking cyberattackers would be observed. Given it is unlikely that prosecutors and investigators would distinguish by cyberattacker motive, if

bare indictments can achieve norm-setting general deterrence against prestige-seeking cyberattacks, then the theory predicts that bare indictments would come to be issued almost exclusively against cyberattacks that are motivated by profit-seeking. This theoretical prediction aligns with the trend of profit-seeking cyberattacking activity emanating from China in the years following the September 2015 Xi-Obama cyber agreement.

4.5.1. Explanations for the Trend; Assessments of the Xi-Obama Cyber Agreement

Around 2017-2018, cybersecurity commentators took notice that the Chinese state seemed to be breaching, or at least approaching the grey-area boundaries of breaching (Barrett, December 20, 2018), the cyber agreement entered into by Xi and Obama in September 2015. Analysts argued that this trend in Chinese cyberattacking activity was characterizable as a shift away from cyberattacks carried out to enable "intellectual property theft," and toward cyberattacks with an arguable Chinese national security purpose (Greenberg 2017). To assess these arguments, the exact wording of the September 2015 agreement is crucial; the relevant provision reads in its entirety, "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" (White House 2015). Cyber policy scholar Herb Lin, writing in *Lawfare* on July 31, 2018, focused on the clause regarding "intent" to show that much cyberattacking activity that could be characterizable as 'international espionage' is

beyond the scope of the provision's prohibitions (Lin 2018). Lin's analysis highlighted that if either party to the agreement "engaged in cyber-enabled theft of intellectual property" for purposes *other than* "providing competitive advantages to companies or commercial sectors," then that party would not be violating the terms of the agreement (Lin 2018).

In an August 11, 2018 assessment for *The Diplomat* entitled "Did the Obama-Xi Cyber Agreement Work?" international relations scholar Robert Farley built upon Lin's analysis. Farley suggested that the 2015 agreement had been successful in combating cyberattacks committed *exclusively* for the purpose of "providing competitive advantages to companies or commercial sectors," but he called attention to an important conceptual feature (Farley 2018). Either party to the agreement could argue that a cyber-enabled theft of "dual-use technology" – intellectual property that had both a commercial use and a national security use – was justifiable; Farley argues, "The United States wanted to reserve for its own intelligence agencies a justification for appropriating foreign military and commercial secrets for national security purposes" (Farley 2018). Indeed, a 2017 analysis by Greenberg quotes the "chief intelligence strategist for security firm FireEye" in contending that China had engaged in cyber-enabled intellectual property theft that was justifiable as dual-use (Greenberg 2017). Further complicating the matter was the challenge of *proving* commercial versus national security intent: "the motivations behind those thefts—and thus any violation of the US-China agreement—are very tough to prove" (Greenberg 2017).

The arguable justifiability of cyber-enabled theft targeting dual-use technology meant that ostensible violations of the agreement could be argued to fall into a grey area.

This was the characterization advanced by an NSA official quoted in a November 2018 report from *Reuters* (Reuters Staff 2018). Likewise, cybersecurity reporter Brian Barrett's December 20, 2018 piece in *Wired* positioned that day's unsealing of the APT10 cyber indictment as indicative of a trend in Chinese cyberattacking activity following the September 2015 agreement: "China has also spent the past few years actively testing the boundaries of the truce, targeting defense contractors, law firms, and other entities that blur the lines between public and private, between intellectual property and more generalized confidential information" (Barrett, December 20, 2018).

The DOJ's February 10, 2020 unsealing of a bare indictment alleging that four PLA officers had violated 18 U.S.C. § 1030 by gaining unauthorized access to the "credit reporting agency Equifax" (DOJ OPA, February 10, 2020) highlighted the dilemma regarding dual-use technology and provided evidence supporting this characterization of the trend in Chinese cyberattacks. Williams – who had coauthored, with Goldsmith, the 2018 *Lawfare* article arguing that bare indictments fail to achieve a deterrent effect – positioned the cyber-enabled theft of personal data as indicative of a trend toward Chinese cyberattacking activity for national security purposes: "If anything, recent developments… demonstrate that the U.S. government is treating personal data more and more as a 'dual use' item with commercial and national-security value alike" (Williams 2020). Williams cited the February 2020 bare indictment to further challenge the contention that bare indictments could have any norm-setting general deterrent effect: "Even if norm construction were the objective, the Equifax allegations do not obviously breach a standard that the United States has embraced. The 2015 U.S.-China agreement did not mention hacking for national-security purposes" (Williams 2020).

I respond to Williams' challenge by arguing that the observable norm-setting is not from commercial purpose to national security purpose – the two sides of the "dual-use" term – but rather from the status-seeking motive to the profit-seeking motive. The reason why the Equifax case is especially puzzling is that the cyber-enabled theft in that case did not seem to have a clear national security purpose. Unlike the cyber-enabled data theft of technological designs and business strategy communications in the PLA Unit 61398 case, the cyber-enabled data theft in the Equifax case was of "personally identifiable information" (*Wu Zhiyong* indictment, line item 2); the indictment alleges, "The PLA hackers obtained names, birth dates, and social security numbers for the 145 million American victims, in addition to driver's license numbers for at least 10 million Americans stored on Equifax's databases. The hackers also collected credit card numbers and personally identifiable information belonging to approximately 200,000 American consumers" (*Wu Zhiyong* indictment, line item 3). Considering that the data was not stolen from a governmental agency, any national security purpose this data could have is attenuated rather than direct, and any national security purpose pales in comparison to the potential economic value of this data.

While this does not mean that the characterization of personal data as dual-use is invalid, I would argue that the taking of a wide-ranging cache of personal data evinces a profit-seeking motive. Indeed, the February 10, 2020 public remarks from U.S. Attorney General William P. Barr – which Williams (2020) directly quotes as evidence for the dual-use characterization – present "economic value" as the more salient feature of the Equifax personal data, and do not expressly allege any national security purpose (Barr 2020). Technological data and personal data may each be characterizable as dual-use, but the

trend in Chinese cyberattacking activity is not toward the national security purpose. Rather, it is toward targeting data whose economic value is more salient than its prestige value. The Equifax case is indicative of a Chinese shift toward the profit-seeking motive.

4.5.2. Proof of Norm-Setting and General Deterrence: The Shift from Prestige-Seeking to Profit-Seeking

An examination of the next nine 18 U.S.C. § 1030 bare indictments issued against Chinese nationals and publicly announced after the PLA Unit 61398 bare indictment further illustrates that this trend is toward profit-seeking.

The next 18 U.S.C. § 1030 bare indictment, which was issued against a Chinese national named Su Bin, was on August 15, 2014 publicly announced. According to a piece by *Wired*'s Garrett M. Graff, there is evidence that U.S. policy practitioners strategically issued this indictment to strengthen bare indictments' deterrent force by demonstrating that bare indictments can lead to arrests (2018). Graff writes that Carlin, the aforementioned U.S. assistant attorney general for national security, had "lamented" to another federal prosecutor that the bare indictment issued against the PLA Unit 61398 officers would almost certainly remain bare; Carlin mused that the next 18 U.S.C. § 1030 indictment issued against a foreign national would be a greater deterrent if there were a high probability that the bare indictment would not remain bare and would instead lead to an arrest (2018). Graff implies that the other prosecutor raised the possibility of issuing the next bare indictment against Chinese national Su, who was more likely to be arrested and face trial because he was currently in Canada, where he was using the name "Stephen"

and leading the life of a wealthy aerospace businessman (2018). A federal criminal complaint, which is another type of criminal charge, was filed against Su on June 27, 2014 (*Su Bin* criminal complaint); even though a bare indictment had not yet been issued, the criminal complaint enabled a provisional arrest warrant to be issued against Su (U.S. Attorney's Office for the Central District of California 2014). Thus, on the day that the bare indictment was announced to have been issued against Su, he was already in custody in Canada (U.S. Attorney's Office for the Central District of California 2014) and awaiting extradition to the U.S. Interestingly, in February 2016, Su waived extradition and surrendered himself to U.S. law enforcement (Garrett 2018). Garrett's description highlights how the informal sanctions associated with apprehension can be contemplable risks that influence a cyber adversary's decisions: "[Su Bin's] lawyer later told a US court that Su Bin knew that his extradition proceedings might last longer than the time he'd serve in a US prison" (Garrett 2018). On February 17, 2016, Su signed a guilty plea that was filed with the U.S. District Court for the Central District of California on March 22, 2016 (*Su Bin* plea agreement).

The text of the indictment, which is appended to Su's plea agreement, shows that the cyberattacks in which Su participated were primarily motivated by prestige-seeking. The intellectual property that Su obtained via unauthorized access and sent back to co-conspirators in China contributed to both scientific advancement and business development. The data was taken from Boeing, an aerospace technology company (*Su Bin* plea agreement, 28). In particular, Su took designs for military aircraft (*Su Bin* plea agreement, 28). According to Graff, U.S. authorities strongly suspected Su of being a spy for the Chinese state (2018). Thus, when the nature of the target and the targeted data is read

in conjunction with this detail implying that Su was carrying out his cyberattacks on behalf of the Chinese state, the information shows that Su had been using cyberattacks to take data directly connected to what the Chinese state sees as markers of prestige.

The next indictment, issued on September 23, 2017 and publicly announced on November 27, 2017, described a shift over time from status-seeking to profit-seeking by the very same cyberattackers. The indictment alleged that the three defendants were members of Boyusec, which "purported to be a Chinese cybersecurity firm" (*Wu Yingzhuo* indictment, line item 1.b.). According to the indictment, between 2011 and January 2014 the defendants used cyberattacks to take "proprietary and confidential economic analyses" (*Wu Yingzhuo* indictment, line item 14). It seems that this data could have been utilized for business development, so the cyberattackers' motivations between 2011 and January 2014 were arguably primarily prestige-seeking. The indictment did not mention the monetary value of this data. January 2014 is prior to the May 2014 publicization of the PLA Unit 61398 bare indictment.

By December 2015 – which, it bears noting, is after the May 2014 publicization of the PLA Unit 61398 bare indictment – the defendants seemed to have shifted to mixed profit-seeking and prestige-seeking. Admittedly, the overlap between business development as a marker of Chinese national prestige and business development as a revenue-generating activity means that it is difficult to make a clear distinction between profit-seeking and prestige-seeking in alleged Chinese cyberattacks. Some evidence is suggested, however, by the wording of the indictment. Although the "technical, design, and business marketing documents" the defendants allegedly took between December 2015

and January 2016 could also have been used for business development if the documents were tendered to the Chinese state, the indictment presented as salient the fact that the data stolen between December 2015 and January 2016 could be valued at "millions of dollars" (*Wu Yingzhuo* indictment, line item 20; line item 28).

On October 30, 2018, the DOJ OPA publicly announced that a bare indictment had been issued against ten members of the Jiangsu Province Ministry of State Security ("JSSD"), a Chinese governmental intelligence entity, for alleged violations of 18 U.S.C. § 1030. The cyberattacks in this case were likely primarily prestige-seeking, since the defendants worked for the Chinese state and the aerospace technological design data taken is comparable to that taken in the PLA Unit 61398 case (DOJ OPA, October 30, 2018). The alleged time range of these cyberattacks, however, is notable. Even though the indictment was not issued and publicized until October 2018, the JSSD cyberattacks allegedly occurred between January 2010 and May 2015 (*Zhang Zhang-Gui* indictment, line item 8). Thus, the JSSD's prestige-seeking cyberattacks predate the Boyusec cyberattackers' apparent shift to profit-seeking.

The fourth § 1030 bare indictment against Chinese nationals that was publicized after the PLA Unit 61398 bare indictment was the APT10 bare indictment, publicly announced on December 20, 2018. This was the bare indictment that prompted Barrett's December 20, 2018 analysis showing that China was operating in a grey area. While the indictment alleges that the APT10 cyberattackers, who were allegedly working with Chinese governmental intelligence, were taking data from a "diverse array of commercial activity, industries, and technologies" (*Zhu Hua* indictment, line item 3.b.), one set of data

stands out as having almost no prestige value if taken: "the personally identifiable information of more than 100,000 Navy personnel" (line item 3.c.). Despite this allegation's consistency with the characterization that the Chinese state has shifted to cyberattacks with a national security purpose, this allegation also supports my contention that the more determinative way to define the shift is from prestige-seeking to profit-seeking. The targets and the targeted data described in the indictment demonstrate that APT10 cyberattackers primarily held mixed profit-seeking and prestige-seeking motives.

The first case representative of purely profit-seeking motives by Chinese cyberattackers was the bare indictment issued against two Chinese nationals, one whose identity was known and one whose identity was unknown, on May 07, 2019. This indictment, whose unsealing was publicly announced on May 09, 2019, described cyberattacks against the medical insurance company Anthem. Although Anthem is a business, the type of data the cyberattackers targeted was not business strategy data that could aid in advancing the Chinese state's prestige. Neither did this data have any national security purposes beyond attenuated ones. Rather, the indictment alleges a theft of personally identifiable information, for which economic value is the most salient feature; as line item 14.c. alleges, "Defendants identified and ultimately stole data concerning approximately 78.8 million persons from Anthem's computer network, including names, health identification numbers, dates of birth, Social Security numbers, addresses, telephone numbers, email addresses, employment information, and income data" (*Wang Fujie* indictment, line item 14.c.). While the monetization of this data could have funded national security operations, that is conceptually distinct from having a national security purpose.

Any prestige-seeking or national security goals that this personal data could ultimately facilitate would have to be accomplished via leveraging its economic value.

An objection is that there was no allegation of state sponsorship in the Anthem case, so it could not have been expected to have a state prestige-seeking motive or national security purpose. However, the next bare indictment did allege Chinese state involvement. By the time the next bare indictment – the aforementioned Equifax case – was issued in January 2020 and unsealed in February 2020, Chinese cyberattackers' shift from primarily prestige-seeking to primarily profit-seeking was complete. As argued above, and like in the Anthem case, there is no direct national security purpose to taking a cache of ordinary American civilians' personal data, and yet the Equifax data was allegedly taken by Chinese governmental actors, members of the PLA. The nation-state utilization of this data hinged on monetization, ergo these cyberattacks allegedly perpetrated by the PLA were primarily motivated by profit-seeking.

The July 21, 2020 press release describing the 18 U.S.C. § 1030 bare indictment filed against two Chinese nationals on July 07, 2020 expressly mentions the "profit" motive of the two defendants (DOJ OPA, July 07, 2020). The indictment alleges that the two defendants took for themselves – not for the benefit of the Chinese state's objectives, whether those goals pertained to prestige-seeking, national security, or otherwise – "hundreds of millions of dollars' worth of trade secrets, intellectual property, and other valuable business information" (*Li Xiaoyu* indictment, line item 3). While this information shows that the defendants were primarily motivated by profit-seeking, they could also be characterized as primarily motivated by both profit-seeking and prestige-seeking. The

indictment alleges that the two defendants sometimes carried out cyberattacks to take, at the behest of a Chinese governmental intelligence agency, "information of obvious interest" to the Chinese state (*Li Xiaoyu* indictment, line item 4). As alleged in the indictment, this information was technological design data; this data directly contributes to scientific advancement, which the Chinese state considers a marker of prestige. However, whether or not prestige-seeking motivated the two defendants, it cannot be denied that they were motivated by profit-seeking for their own personal financial enrichment.

The eighth and ninth bare indictments, collectively indicting five Chinese nationals who were thought to be part of a cyberattacking group called APT41, were announced together. The eighth was issued in August 2019 against three Chinese nationals and the ninth in August 2020 against two Chinese nationals, but the indictments' public announcement came on September 16, 2020. These bare indictments were announced in conjunction with an indictment that accused two Malaysian nationals, in connection with APT41, of having violated 18 U.S.C. § 1030; the indictment against the Malaysian nationals is not a bare indictment, since Malaysia does have a bilateral extradition treaty with the U.S. and the two Malaysian individuals were indeed arrested by Malaysian law enforcement officials "on Sept. 14, 2020, pursuant to a provisional arrest warrant from the United States" (DOJ OPA, September 16, 2020). The eighth and ninth bare indictments alleged a conspiracy to gain unauthorized access to the computer systems of a video game company; this target indicates primarily profit-seeking motives. Correspondingly, the threat of bare indictment had not achieved a general deterrent effect against the APT41 members, and bare indictments' issuance against them also did not achieve a specific deterrent effect. Note that, unlike how the national security purpose would be a motive of nation-state

actors rather than nonstate actors, the salience of the profit-seeking motive is irrespective of whether APT41 is categorized as a nation-state actor. This case shows that even nation-state actors can cyberattack for profit. Furthermore, just as the theory predicts, the issuance of the bare indictments against the APT41 members in 2019 and 2020 failed to deter these profit-seeking actors from committing recidivist cyberattacks. As recently as March 08, 2022, Mandiant was publishing a technical attribution report (Brown et al. 2022) on the continuing cyberattacks committed by APT41. Mandiant described APT41 as a nation-state actor that was primarily motivated by profit-seeking: "APT41 is a prolific Chinese state-sponsored espionage group known to target organizations in both the public and private sectors and also conducts *financially motivated activity for personal gain* [emphasis added]" (Brown et al. 2022). While Mandiant's description of APT41 does resonate with a shift to a national security purpose, it also provides evidence for the contention of a shift to profit-seeking.

Consistent with theoretical predictions, these brief case studies show that bare indictments against Chinese nationals have, in the time between 2014 and 2020, become issued exclusively against cyberattackers who are primarily motivated by profit-seeking or who are primarily motivated by mixed prestige-seeking and profit-seeking; it is as though the presence of a profit-seeking motive enables the presence of other motives. In turn, this analysis evidences that the bare indictment achieved a norm-setting general deterrent effect.

The norm set was not, as many scholars believe, a disallowance of commercial gain and a condoning of the national security purpose. Although this was the norm recorded in

the 2015 Xi-Obama agreement, the trend in Chinese cyberattacking activity did not proceed in accordance with this distinction. The Equifax cyberattacks had little to no national security purpose, and yet they were allegedly executed by Chinese nation-state actors. The Equifax case shows that even nation-state actors shifted to profit-seeking motivations.

Irrespective of whether Chinese nationals are nation-state actors or nonstate actors, they now follow the general norm that has been set: Do not commit, or attempt to commit, cyberattacks that are primarily motivated by prestige-seeking and are not primarily motivated by profit-seeking. The fear of the consequences – a bare indictment's denial of status – has, evidently, been sufficient to achieve general deterrence against Chinese prestige-seeking cyberattacks. Hence, bare indictments' effectiveness as a general deterrent measure against prestige-seeking cyberattacks perpetrated by Chinese nationals predicts and explains the trend in Chinese cyberattacking activity, as the deterrence of prestige-seeking has led to the salience of profit-seeking cyberattacks perpetrated by Chinese nationals who are then indicted under § 1030.

4.6.0. Iranian Cyberattackers' Shift to Mixed-Motive Profit-Seeking Cyber Espionage Operations

Since 2019, the publicized bare indictments issued by the U.S. against Iranian nationals reveal a similar trend toward politically driven cyber intrusions that include profit-seeking motives. This section centers on the discussion of 18 U.S.C. § 1030 bare indictments issued against Iranian nationals since 2019. First, I use the case study of Monica Witt and the Cyber Conspirators to introduce a seeming trend toward politically

driven 'espionage operations.' Ultimately, however, I suggest that just as the Chinese trend was better characterized as being toward profit-seeking motives rather than toward the national security purpose, the Iranian trend is better characterized as being toward profit-seeking motives rather than toward political purposes. The details of the Witt and the Cyber Conspirators case study indicate that the deterrent effect of bare indictment may have been split in accordance with the different motives of the accused cyberattackers. While evidence indicates that one of the defendants was primarily motivated by prestige-seeking, analysis shows that the other four defendants were motivated by profit-seeking. As the apparently prestige-seeking defendant has ceased her cyberattacking behavior but the arguably profit-seeking defendants have been obviously undeterred even after the publicization of a bare indictment against them all, this case study provides evidence that aligns with the theory's predictions. Next, I discuss a separate indictment that had been publicized against one of the defendants in this case, which shows that a cyberattacker's motives can change over time; this provides an empirical illustration of the theory's hypothetical on motive shifting. Finally, to further establish the Iranian trend toward mixed-motive profit-seeking, I discuss the remaining publicized 18 U.S.C. § 1030 bare indictments against Iranian nationals.

4.6.1. Profit-Seeking Operatives Undeterred, but Prestige-Seeking Operative Possibly Deterred [IRAN-07]

Since 2019, the schemes that are described in unsealed indictments alleging violations of 18 U.S.C. § 1030 by Iranian nationals have seemingly been indicative of Iranian nationals' increasing use of cyberattacks to accomplish politically motivated cyberattacks,

including what I will refer to as "espionage operations." I define this term as operations whose success is dependent on the concealment of the operative's identity as a foreign agent.[16] However, I argue that the more consistent way to characterize the trend is toward profit-seeking.

For background information, note the various motives exhibited in the case studies involving publicized § 1030 bare indictments issued against Iranian nationals prior to 2019. The Arrow Tech case study, involving indictments publicized in 2015 and 2017, is discussed in Chapter 6 and is an arguable example of indeterminate, mixed motives. The U.S. Financial Industry DDoS case study, wherein the relevant indictment was issued in 2016, is discussed in Chapter 8 and is arguably dominance-seeking. In Chapter 6, I argue that the cyberattacks in the Mabna Institute case study, involving an indictment publicized in 2018, were motivated by prestige-seeking. The thrill-seeking motives of the SamSam Ransomware case study are discussed earlier in this chapter.

On February 13, 2019, the DOJ OPA publicly announced the unsealing of an indictment charging an American citizen and four Iranian alleged co-conspirators with multiple violations of 18 U.S.C. § 1030. The indictment described that the American citizen, former U.S. Air Force intelligence officer Monica Witt, had defected to Iran in 2013; the four Iranian nationals, which the indictment refers to as the "Cyber Conspirators," were affiliates of an Iranian entity that "conducted malicious computer intrusions on behalf of the IRGC" (*Witt* indictment, 9). "IRGC" refers to "Islamic Revolutionary Guard Corps," a

[16] I do not use the term "espionage" in a legal sense; my use of the term "espionage" to describe certain activities should not necessarily be taken to assert violations of the U.S.'s Espionage Act of 1917 (18 U.S.C. §§ 792-799) or other applicable law. Likewise, I do not use the term "foreign agent" in a legal sense. However, based on the information in the indictments, the argument can often be made that some of the persons whom I implicitly or explicitly characterize as "foreign agent" meet the legal definition of "agent of a foreign principal" under the U.S.'s Foreign Agents Registration Act of 1938, 22 U.S.C. § 611(c)(1)(i).

branch of the Iranian military (*Witt* indictment, line item 4). The indictment alleged that Witt disclosed to Iranian government officials information that the Cyber Conspirators used to attempt unauthorized access of protected computers used by U.S. government intelligence; for example, Witt provided the name of a U.S. government agent whom the Cyber Conspirators subsequently targeted (*Witt* indictment). The Cyber Conspirators did so by concealing their true identities as foreign agents. With Witt having provided the U.S. government agent's "true name," in 2015 the Cyber Conspirators allegedly sent malware to the personal – as opposed to professional – accounts of this U.S. government agent and seven other U.S. government agents (*Witt* indictment). These malware links and malware files, if opened by the recipient, "would have provided the Cyber Conspirators with covert, persistent access" to any computer network that the recipient's computer accessed, including U.S. government computer networks (*Witt* indictment, 20).

Based on the information in the indictment, all five of the defendants can be characterized as operatives in an espionage operation. However, notwithstanding that they were all operatives in the same intelligence operation, their motives were different; while it appears Witt was primarily prestige-seeking, it seems the Cyber Conspirators were primarily profit-seeking.

A February 16, 2019 article from the *New York Times* covering Witt's defection portrays her as angry with American foreign policy and infatuated by Iranian culture. Cory Ellis, a classmate who spoke to the *New York Times*, described Witt's indignation at academic arguments critical of Iran, as exemplified by the capstone presentation Witt gave for her master's degree program: Ellis "recalled Ms. Witt's argument as a 'love letter to Iran,' and said she asserted that the country would only use a nuclear weapon in self-

defense. Faculty members hit her hard with questions, Mr. Ellis recalled, and Ms. Witt appeared to shrink in response. 'She was almost offended that the assumption that Iran was a peace-loving nation would even be questioned,' he said. 'She was visibly upset'" (Blinder et al. 2019).

Witt's attempts to raise others' view of Iran's status support the contention that Witt's motives for engaging in these cyberattacks were primarily prestige-seeking. In accordance with the prediction that the bare indictment would deter Witt from committing further cyberattacks, open-source research does not yield any new information on Witt's activities, cyber or otherwise, since the unsealing of the bare indictment. In the package of informal sanctions that was triggered by the bare indictment, the bare indictment could have deterred Witt from recidivist cyberattacks by lowering her expected weighted benefit. Exposing the espionage operations she carried out on behalf of the Iranian state would tend to deny the objective of prestige that she arguably sought on behalf of Iran. By attributing these cyberattacks to Witt, the bare indictment communicated to Witt that her ideological positions would hold little credence to others. Thus, the bare indictment not only frustrated her objective, but also made any further attempts less likely to succeed.

Counterarguments against the bare indictment's deterrent effect on Witt could be made by pointing out that – in the years between the cyberattacks in 2015 and the indictment's unsealing in 2019 – Witt could simply have become disinclined to commit further espionage-related cyberattacks, or Witt could have run out of information that would have been useful to the Iranian state. The first of these premises could be true, but it seems unlikely in light of Witt's apparent devotion to prestige-seeking on behalf of Iran. As for the second of these premises, the indictment indicates that Witt's role in the espionage

operation was not limited to her knowledge of classified or otherwise protected information. For instance, the indictment alleges that Witt, often seemingly of her own volition and without needing orders from Iranian government officials (*Witt* indictment, 15; Burgess 2019), performed Facebook searches on social media to find U.S. government agents and their family members whom the Iranian state could then target for cyberattacks. Searching on social media is not an activity that requires specialized knowledge or skills, as any individual with a Facebook account could accomplish this simple task in the individual's spare time. If the U.S. government or a private cybersecurity firm were to find and release information that Witt, as a known accused cyberattacker, has continued to support cyberattacks by conducting Facebook searches for U.S. government agents, then such evidence would indicate that Witt has been undeterred; currently, however, there is no evidence that Witt has continued to conduct even this simple task. Still, because the timing of Witt's halt in cyberattacks predated rather than coincided with the publicization of the bare indictment, the evidence that she was deterred by the bare indictment is suggestive rather than dispositive.

Nevertheless, there is no shortage of information indicating that the Cyber Conspirators – who were arguably profit-seeking rather than prestige-seeking – were undeterred by bare indictment. In another example supporting the contention that the absence of information on known cyberattackers is highly unusual in the cyber arena unless such cyberattackers are, in actuality, no longer active, the firms Facebook, Symantec, and Mandiant have – between 2019 and 2021 – released public statements and published information that attribute an Iranian malware campaign to the very same Iranian entity of which the Cyber Conspirators were allegedly affiliates (Greenberg 2021). This Iranian

malware campaign, as described by cybersecurity reporter Andy Greenberg in an article for *Wired*, used essentially the same tradecraft as the scheme described in the indictment; the malware campaign sent malware to the personal accounts of U.S. government agents (Greenberg 2021).

If the four Cyber Conspirators were carrying out cyberattacks as part of an espionage operation on behalf of the Iranian state, why are the Cyber Conspirators better characterized as profit-seeking rather than prestige-seeking? The information in the indictment suggests that the Cyber Conspirators' reason for gaining unauthorized access was to obtain data. As discussed in Chapter 2's definition of "cyberattack," data can be treated as a valuable commodity. Although the indicators of motive in this project's framework can overlap – for instance, the data that the Cyber Conspirators wished to obtain via unauthorized access to U.S. government networks might eventually have been used to gain prestige for the Iranian state – there is no information indicating that the data was particularly regarding specifications for defense materiel, which I will later argue that the Iranian state considers to be markers of prestige; nor that the data was to be otherwise used for prestige-seeking purposes. Rather, it seems that the Cyber Conspirators were to obtain this generalized data on behalf of the Iranian state, and – as could have been done with allocating a cyberattack-enabled taking of monetary funds – the Iranian state would figure out later what operations the data could support.

As predicted, therefore, the informal sanctions triggered upon the publicization of the bare indictment did not deter this profit-seeking cyberattacking activity. The negative consequences in the package of informal sanctions could not outweigh the expectation of profit as it would the expectation of emotional thrill, and unlike how informal sanctions can

directly frustrate prestige-seeking objectives by denying status, nothing in the package of informal sanctions directly frustrates the objective of profit. However, the package of informal sanctions does include an attack on face, which – aligning with predictions – could have deterred status-seeking actors such as the prestige-seeking actor in this case study.

4.6.2. An Iranian National's Shift in Cyberattacking Motive [IRAN-04]

Information from a DOJ press release regarding an earlier § 1030 bare indictment issued against one of the Cyber Conspirators, Behzad Mesri, aligns with the underlying hypothetical on shifting motives. This HBO case study establishes that the very same alleged cyberattacker, over time, can shift to conducting cyberattacks in which different motives are salient.

On November 21, 2017, the U.S. Attorney's Office ("USAO") for the Southern District of New York ("SDNY") announced a § 1030 bare indictment regarding a 2017 cyberattacking "scheme" against the entertainment company HBO (USAO SDNY, November 21, 2017). As described in the press release, the indictment was issued against Iranian national Behzad Mesri, whom the press release expressly identified as a cyberattacker "who had previously worked on behalf of the Iranian military" (USAO SDNY, November 21, 2017). The press release summarized the indictment's allegations that the cyberattacker, upon gaining unauthorized access to HBO's computer systems, took HBO's confidential digital information pertaining to upcoming television shows and then attempted to extort from HBO a ransom of six million USD in exchange for not further disclosing the data (USAO SDNY, November 21, 2017).

Indicia relevant to behavioral analysis of motive show that the cyberattacking scheme against HBO was motivated by mixed profit-seeking and thrill-seeking. For point of comparison, it might be noted that the ransom demand in this case study – six million USD – was roughly equal to the *cumulative* total of the ransom profits in the SamSam Ransomware case study. This apparent focus on monetization of taken data evidences a profit-seeking motive. However, one conspicuous and somewhat bizarre detail regarding a gratuitous taunt the cyberattacker issued against victim HBO is a convincing indicator of thrill-seeking; according to the press release, the ransom demand "concluded with a custom image depicting the 'Night King,' an undead character from [HBO television series] 'Game of Thrones,' and bearing the message, 'Good luck to HBO'" (USAO SDNY, November 21, 2017). Since taunts against the victim of a victim of a cyberattack evince thrill-seeking motives, the cyberattacking scheme against HBO was motivated by mixed thrill-seeking and profit-seeking.

Interestingly, the *Witt* indictment named the same individual, Behzad Mesri, as one of the Cyber Conspirator defendants alleged to be carrying out cyberattacks on behalf of the Iranian military. Although the *Witt* indictment was publicized on February 13, 2019 – two years after the November 2017 publicization of the § 1030 indictment against Mesri – the *Witt* indictment concerned cyberattacking activity that occurred between 2014 and 2015 (*Witt* indictment, line item 51). Even though the *Mesri* indictment was issued before the *Witt* indictment, the cyberattacking scheme that Mesri allegedly mounted against HBO occurred in mid-2017, which is after the 2015 occurrence of the cyberattacking activity described in the *Witt* indictment. With this timeline in mind, the cyberattacking behavior allegedly perpetrated by Mesri indicates that Mesri apparently shifted from profit-seeking

to mixed thrill-seeking and profit-seeking. Since this case study shows that an alleged cyberattacker may shift motives over time, it provides evidence for the theorized mechanism that underlies the predicted issuance of § 1030 bare indictments against cyberattacks motivated by profit-seeking.

4.6.3. An Iranian Shift toward Profit-Seeking in Political Cyberattacks

Alleged Iranian cyberattackers' increasing shift toward profit-seeking motives is further demonstrated by a brief examination of four more publicized bare indictments issued against Iranian nationals. Although an implication is that that cyberattacks from Iranian nationals – like cyberattacks perpetrated by Chinese nationals – will now be less likely to be deterred by the issuance and publicization of § 1030 bare indictments, this implication is symptomatic of bare indictments' effectiveness as a deterrent measure against status-seeking and thrill-seeking.

On September 18, 2020, the FBI published an article regarding three separate bare indictments pertaining to three recent cases charging violations of 18 U.S.C. § 1030.

The first indictment was filed on September 03, 2020, and its unsealing was publicly announced by the USAO for the District of Massachusetts on September 15, 2020. The indictment and the press release alleged that a nineteen-year-old Iranian national and a twenty-five-year-old stateless national had violated 18 U.S.C. § 1030 by gaining unauthorized access to U.S. websites and defacing the websites with anti-American, pro-Iranian statements (USAO District of Massachusetts, September 15, 2020). As the indictment and the press release described these individuals as acting out of anger over the "United States military action in January 2020 that killed Qasem Soleimani, the head of the

Islamic Revolutionary Guard Corps-Quds Force, a U.S.-designated foreign terrorist organization" (USAO District of Massachusetts, September 15, 2020), the individuals' motives could best be described as dominance-seeking. An indication of dominance-seeking motives is the use of the cyberattacks in disseminating menacing messages that attempted to undermine the U.S. Because dominance-seeking is a means of status-seeking and a bare indictment denies status, it is likely that the bare indictment will have specifically deterred the dominance-seeking alleged cyberattackers from committing further cyberattacks.

The second indictment, the unsealing of which was announced by the USAO for the District of New Jersey on September 16, 2020, is also likely to have deterred the two Iranian individuals against whom it was issued, because these two individuals arguably had status-seeking motives. As described in the press release and the indictment, these two individuals stole intellectual property primarily pertaining to specifications on aerospace defense materiel (USAO District of New Jersey, September 16, 2020), which the Iranian state regards as markers of prestige. Similar to the two individuals named in the first indictment, these two individuals also defaced many U.S. websites with "images of burning Israeli flags and threats forecasting the death or demise of citizens in the United States, Israel, and elsewhere" (USAO District of New Jersey, September 16, 2020). The taking of markers of prestige indicates prestige-seeking, and the defacement of U.S. websites indicates dominance-seeking; as these motives are both means of status-seeking, a deterrent effect was likely achieved by the bare indictment.

The third indictment was filed on September 15, 2020, and its unsealing was announced by the USAO for the Eastern District of Virginia on September 17, 2020. The

indictment and press release alleged that three Iranian nationals acting on behalf of the IRGC had obtained unauthorized access to the computer systems of "aerospace and satellite tracking companies" "in order to steal critical information related to United States aerospace and satellite technology and resources" (USAO Eastern District of Virginia, September 17, 2020). This is arguably a mixed profit-seeking and prestige-seeking case, but some indicia point to the predominance of prestige-seeking. Despite the espionage-related phishing and malware tradecraft in this case being similar to the tradecraft used by the Cyber Conspirators, prestige-seeking motives are evidenced by the targeting of aerospace "data sought by the IRGC" (USAO Eastern District of Virginia, September 17, 2020) rather than a wide-ranging cache of data for an undetermined purpose. On the other hand, the press release's characterization of the taken intellectual property as carrying high economic value leans toward profit-seeking. As with how the overlap in business development data as a Chinese marker of national prestige and as an asset that carries high economic value lent some ambiguity to whether the Boyusec case study involved profit-seeking or prestige-seeking, the overlap between aerospace defense data as an Iranian marker of national prestige and aerospace defense data as an economically valuable asset means that a profit-seeking element is arguably also at play here. Since dominance-seeking is less prominent here than in the previous case studies, however, the bare indictment in this third case shows lesser promise for having deterred the indicted cyberattackers.

A fourth case study shows why politically driven espionage operations are not *per se* more difficult to deter, but rather, are more difficult to deter when they contain profit-seeking motives. On November 18, 2021, the DOJ's OPA and the USAO's SDNY announced the unsealing of an indictment charging two Iranian nationals, who were at the time

twenty-four and twenty-seven years old respectively, with violations of 18 U.S.C. § 1030 in connection with a "Cyber-Enabled Disinformation and Threat Campaign Designed to Interfere with the 2020 U.S. Presidential Election" (USAO SDNY, November 18, 2021). As described in the press releases and the indictment, these two individuals – Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian – had attempted to obtain unauthorized access to state voting websites and the computer network of a media company so that they could have "another vehicle for further disseminating false claims" regarding the election (USAO SDNY, November 18, 2021). Since the success of this operation was dependent on making victims believe that the disinformation originated from U.S. official entities rather than foreign agents, it was an espionage operation. Via unauthorized access, the individuals obtained a wide-ranging cache of "confidential U.S. voter information" that was then used for a specific purpose: to "intimidate and influence American voters" (DOJ OPA, November 18, 2021; *Kazemi* indictment). As this case presents an example of mixed profit-seeking and dominance-seeking, it is predicted to be more difficult to deter. Indeed, despite – or perhaps because of[17] – Kazemi's and Kashian's being added to the SDN List alongside their employer Emennet Pasargad and four other employees of Emennet Pasargad on the same day as the indictment's unsealing (DOJ OPA, November 18, 2021), an Iranian Foreign Ministry spokesman immediately "condemned the new sanctions as illegitimate" (Iran Primer 2021), and Emennet Pasargad has been undeterred from mounting further cyberattacks. As recently as January 2022, the FBI issued advisories warning of the active cybersecurity threat posed by Emennet Pasargad

[17] See Chapter 6's discussion of the Mabna Institute case study for an argument on why simultaneous imposition of economic sanctions alongside the issuance of a bare indictment can counterproductively undermine the deterrent effects of bare indictment.

and providing recommendations on how to strengthen cybersecurity defenses (FBI, January 26, 2022).

These cases suggest that bare indictments are less likely to achieve a specific deterrent effect against cyberattack-enabled espionage operations not necessarily because 'political' cyberattacks are *per se* more difficult to deter, but because the package of informal sanctions triggered by bare indictment do not directly counteract the profit-seeking component when a cyberattacker's motives for mounting a political cyberattack involve profit-seeking. The effects can be distinguished because there is no evidence to indicate that Witt, a primarily prestige-seeking accused cyberattacker in an alleged Iranian government espionage operation against the U.S. government, has continued mounting cyberattacks; by contrast, the primarily profit-seeking Cyber Conspirators were obviously undeterred. Moreover, the cyberattackers in the case studies regarding political defacement of U.S. websites probably held a very high expected weighted benefit in terms of quantity, but my discussion shows that they can nevertheless have been deterred by bare indictment because the informal sanction of an attack to face directly denies the quality of the expected benefit of status, bringing the value of *B* down to near 0 and resulting in a low expected weighted benefit. The overall trend in § 1030 bare indictments issued against Iranian nationals is toward profit-seeking, which implies that § 1030 bare indictments will be less likely to achieve deterrent effects against cyberattacks allegedly perpetrated by Iranian nationals henceforth, but also aligns with the predictions of the theory.

///

4.7. The APT40 Indictment and An International Coalition's Failure to Deter [XNA-11]

As discussed in Section 4.2. and Section 4.5., bare indictments – domestic criminal charges – achieved specific deterrence against prestige-seeking Chinese nation-state actors and hence achieved general deterrence by setting a norm regarding the expectation of punishment: Chinese cyber adversaries could expect that the U.S. would issue indictments against suspected cyberattackers. With the punishment of indictment being the expectation, whether bare indictments deterred potential Chinese cyberattackers became dependent on whether the denial of prestige lowered expected benefit. This explains the shift to bare indictments against Chinese actors motivated by profit: even when profit-seeking actors expect that indictments will be issued against them, the package of informal sanctions neither directly frustrates nor indirectly outweighs the expected benefit of profit in the cost-benefit calculus. Against prestige-seeking actors, bare indictments' deterrent value stems primarily from their ability to label suspected offenders "criminal outcasts"; the case study of the PLA Unit 61398 officers examined the functions of indictments to explain why accusing someone of violating the criminal law is a far more effective 'shaming' mechanism than accusing someone of violating something akin to the civil law. While committing an offense considered to be squarely within the civil law – breach of contract, for instance – is not necessarily incompatible with holding a high status, being labeled a *criminal outcast* is inherently inconsistent with having prestige in a mainstream social hierarchy such as the international order. The only prestige one might gain from such a label is prestige among a society of fellow criminals, which – as shown by an examination of Chinese foreign policy goals – is clearly not the type of 'prestige' that the Chinese state seeks.

The relative inefficacy of civil law – or, rather, communicative actions that accuse someone of a violation more akin to the civil law than the criminal law – as a shaming measure is brought to light by a recent development in international diplomacy regarding the technical attribution of the Chinese state as the perpetrator of widespread cyberattacks. I use the discussion of this case study to highlight the distinction between civil naming-and-shaming and criminal naming-and-shaming. As my analysis shows that the additive cumulation of civil naming-and-shaming by an international coalition failed to achieve a deterrent effect against prestige-seeking actors, this case study analysis supports the argument that the package of informal sanctions triggered by bare indictment deters due to the accusation of *criminal* social deviance, rather than just social deviance generally.

On July 19, 2021, the government of the United Kingdom ("UK") released public statements of attribution regarding a worldwide intrusion of Microsoft Exchange Servers, attributing these cyberattacks to the Chinese state (National Cyber Security Centre, July 19, 2021). Specifically, the UK accused the Chinese Ministry of State Security ("MSS") of backing a group of cyberattackers known in the cybersecurity community as APT40, short for "Advanced Persistent Threat 40." Just as the U.S. Department of Justice is the U.S. government agency that usually issues press releases regarding the unsealing of indictments, the UK's 2021 public statements were made by two UK government agencies: the UK's National Cyber Security Centre and the UK's Foreign, Commonwealth & Development office (National Cyber Security Centre, July 19, 2021; Foreign, Commonwealth & Development Office, July 19, 2021). Unlike how the publicly announced unsealing of a U.S. bare indictment usually stands alone as a governmental action taken by one nation-state, however, the UK's 2021 public statement was part of coordinated action

amongst international allies (Lonergan 2021). International affairs scholar Erica Lonergan, in an analysis for the *Carnegie Endowment for International Peace*, lists the eight allies – six nation-states and two international organizations – that simultaneously "issued similar statements" on July 19, 2021: the European Union ("EU"), the North Atlantic Treaty Organization ("NATO"), Japan, the UK, the U.S., Australia, Canada, and New Zealand (Lonergan 2021). The latter five countries are the five members of the so-called "Five Eyes" intelligence alliance. J. Vitor Tossini's descriptive brief for the *UK Defense Journal* describes the origins of the Five Eyes as an information-sharing coalition between corresponding intelligence agencies from likeminded nation-states: "The Five Eyes was formally founded in the aftermath of the Second World War, through the multilateral agreement for co-operation in signals intelligence, known as the UKUSA Agreement, on 5 March 1946" (Tossini 2020).

Of the nation-states that publicly attributed and 'shamed' China, it seems that only the U.S. issued domestic criminal charges. On July 19, 2021, the DOJ's OPA publicly announced the unsealing of an indictment accusing four Chinese nationals of being members of APT40 and therefore of violating 18 U.S.C. § 1030 on behalf of the Chinese government. The text of the indictment even purported to unmask the true identity of the cyberattacker group that the cybersecurity community had referred to as APT40. APT40, the indictment alleged, was Hainan Xiandun, a "front company" which had been created by the Hainan Province branch of the MSS. The information included in the indictment (*Ding Xiaoyang* indictment) and summarized by the press release supports an argument that the cyberattackers were primarily prestige-seeking, since their cyberattacks were used to

support China's prestige-related goals of scientific advancement and business development.[18]

With the cyberattackers being clearly motivated by prestige-seeking, this project's theory would predict that the bare indictment would have a deterrent effect. The communicative action of the bare indictment's unsealing, however, was overshadowed by a statement issued by the U.S. White House and by the statements issued by the other allies. Proof of this contention regarding overshadowing comes by looking to analyses and news reports from the U.S. and the UK. Lonergan's analysis leads with the White House's statement, and only mentions the indictment further down in the body of the analysis. The *Guardian*, a UK-based independent news company, expressly highlights the U.S.'s involvement in the coordinated actions of July 19, 2021 and quotes the White House statement (Sabbagh et al. 2021), but makes no mention of the U.S.'s issuance of domestic criminal charges against APT40 members. *U.S. News*' analytical report from national security correspondent Paul D. Shinkman not only ignores the press release that publicly unsealed the indictment, but also seems to exclude that DOJ public statement's existence from the group of coordinated actions taken among the allies. The press release could fairly be characterized as a statement that offered details about the APT40 cyberattacks, yet Shinkman writes, "But in some ways, the comments were most notable for what they

[18] "Targeted industries included, among others, aviation, defense, education, government, health care, biopharmaceutical and maritime. Stolen trade secrets and confidential business information included, among other things, sensitive technologies used for submersibles and autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, proprietary genetic-sequencing technology and data, and foreign information to support China's efforts to secure contracts for state-owned enterprises within the targeted country (e.g., large-scale high-speed railway development projects). At research institutes and universities, the conspiracy targeted infectious-disease research related to Ebola, MERS, HIV/AIDS, Marburg and tularemia" (DOJ OPA, July 19, 2021).

didn't do. Specifically, the statements themselves and officials speaking privately to explain them would not offer any details about the ransomware attacks" (Shinkman, July 19, 2021).

The coordinated statements did – as Shinkman's *U.S. News* piece shows – prompt an indignant response from the Chinese state. However, analyzing the tone of the response's translated text shows that, rather than achieving deterrence, these coordinated statements could have been escalatory and hence counterproductive. Unlike China's immediate response to the U.S.'s 2014 bare indictment against the PLA Unit 61398 officers, China's immediate response to the allies' coordinated statements was not only indignant, but enraged. Shinkman writes on July 19, 2021, "Beijing called the claims 'a huge lie,' 'slander' and 'ridiculous,' and it threatened devastating consequences…, according to a post in China's English-language Global Times, considered a mouthpiece for the Chinese Communist Party" (Shinkman, July 19, 2021). Shinkman further quoted the Chinese post as threatening to "retaliate" (Shinkman, July 19, 2021).

The content of this infuriated response can be contrasted with the points of the official statement issued by Chinese government spokesperson Qin in the PLA Unit 61398 case. In this APT40 case, the unofficial response from the Chinese state did include a direct denial of the cyberattacking behavior itself. Moreover, unlike how Qin's statement threatened a cessation of diplomatic relations between the U.S. and China, the response here threatened an act of escalatory retaliation – a move that is directly contrary to deterrence. Along with the unofficial rather than official nature of the Chinese state's response, the use of the word 'retaliation' suggests that China interpreted the international coalition's condemnations not as an accusation of criminality, but rather as dominance-

seeking actions themselves: strong-arm tactics, from parties on roughly equal footing with China, to pressure China into compliance irrespective of the social norms of the global order. Overall, then, the content of the Chinese state's response in the APT40 case evidences an argument that the deterrent effect of the international coalition's statements was suboptimal. I suggest that the suboptimality stems from the civil rather than criminal nature of the international coalition's condemnations.

With the strength of two international organizations and six nation-states, these coordinated actions of diplomatic communication among allies naming and shaming China might have been predicted to have a far stronger deterrent effect than would a U.S. bare indictment alone as a means of naming and shaming. Instead, the allies' statements apparently infuriated China, so the overall effect may have been counterproductive. I argue that the reason for this difference lies not just in the extent of the shaming, but also in the quality of the shaming. In the case study of the PLA Unit 61398 indictment, I argued that although the label of "criminal outcast" is essentially a shaming mechanism among the package of informal sanctions, labeling someone a "criminal outcast" is far more effective than other forms of naming and shaming. If the effectiveness of naming and shaming were solely a matter of extent – of international cooperation in shaming, as David Hechler (2021) suggests – then a "coalition" of many parties shaming would be expected to have an enhanced norm-setting deterrent effect (Hechler 2021). This prediction is not consistent with the Chinese state's enraged response on July 19, 2021. The apparent lack of deterrent effect lies primarily in the quality of the shaming statements that overshadowed the unsealing of the bare indictment; the allies' statements accused the Chinese state of offenses akin to violations of civil law – in particular, breach of contract.

After the September 2015 cyber agreement between Xi and Obama, China had entered into similar formal cyber agreements with other nation-states and with international organizations; Adam Segal, in a piece for the *Council on Foreign Relations*, writes, "A month after signing the agreement with the United States, China inked a similar deal with the United Kingdom, and, in November 2015, China, Brazil, Russia, the United States, and other members of the Group of Twenty accepted the norm against conducting cyber-enabled theft of intellectual property" (Segal 2016). The UK's public statements on July 19, 2021 accused the Chinese state of having broken these agreements; the closing line of the statement from the UK's Foreign, Commonwealth & Development Office reads, "The UK is calling on China to reaffirm the commitment made to the UK in 2015 and as part of the G20 not to conduct or support cyber-enabled theft of intellectual property of trade secrets" (Foreign, Commonwealth & Development Office, July 19, 2021). While the UK did not formally accuse China of breach of contract, as a formal accusation would have been accomplished by initiating a civil suit against the MSS, accusing China of breaking its agreements can be likened to alleging a breach of contract.

Accusing someone of violating the civil law is like accusing them of 'not playing well with others.' Making common knowledge an accusation of 'uncooperativeness,' rather than of criminality, will likely be inefficient as an attack to status. A public accusation that someone is uncooperative is not a very effective deterrent, because being uncooperative is not inconsistent with holding a high rank in a social hierarchy. This theoretical concept is especially true of breach of contract. Breach of contract is firmly located in the civil rather than criminal law (Markovits and Atiq 2021, 1.1). This understanding of contract law is not unique to U.S. jurisdictions, but rather, is a common understanding in legal theory (Bedi

2013); moreover, this understanding is formally codified in Chinese law (Contract Law of the People's Republic of China, Chapter VII, Article 107). Thus, while breach of contract under the civil law might lead to being deemed 'uncooperative,' it does not lead to being deemed a criminal outcast. Indeed, legal theory and the civil law itself implicitly encourage breach of contract under certain circumstances (Markovits and Atiq 2021, 1.1). Theories of "efficient breach" predict that a party can, will, and even *should* commit breach of contract where the party expects that it is less costly and therefore economically efficient for the party to suffer the formal legal consequence of paying monetary damages than it is for the party to keep its commitment under the contract (Markovits and Atiq 2021, 1.1; Legal Information Institute, "Efficient Breach," n.d.; Bedi 2013, 564; Bedi 2013, 567 at footnote 29). As with deterrence, the efficient breach doctrine hinges on the expected cost-benefit calculus of a party. If the Chinese state expected that it would be less costly to bear the consequences of not abiding by its cyber agreements than it would to follow them, then the doctrine of efficient breach could justify the commitment-breaking of which the coalition accused China. The analogy is even stronger when applied to the present situation, where the Chinese state has neither the expectation of informal sanctions nor the expectation of formal legal consequences to prevent it from making an efficient breach of its agreements. By labeling deviant behavior as "criminal," formal charges could have achieved specific deterrence of the alleged Chinese cyberattackers' arguably prestige-seeking goals, and hence have achieved general deterrence upon other potential offenders. Instead, the message sent to the Chinese state was that the worst consequence to fear is being called disagreeable, a trait that – unlike being called an outcast – is not necessarily incompatible with status.

Therefore, because the shaming was civil rather than criminal – and particularly so because the civil law violation that the allies informally accused China of committing was breach of contract, wherein efficient breach is predicted, acceptable, and encouraged – the coordinated statements failed to lower the Chinese nation-state cyberattackers' expected benefit of status. The combined quantity or extent of the shaming may have infuriated China, but the quality or nature of the shaming meant that it was not a direct denial of status and hence was a suboptimal deterrent. General norms are more forcefully, and hence effectively, set by labeling behavior "criminal" than they are by labeling behavior "disagreeable."

Here, where only the U.S. issued domestic criminal charges against APT40 members, analysts and reporters focused on the coalition's condemnations; the indictment's unsealing was minimally covered. This extraordinary development in international cyber diplomacy detracted international attention from the APT40 indictment; where the indictment was covered as an international rather than domestic matter, it was mentioned as only a minor component of the coalition's actions. Analysts' and reporters' minimizing and being distracted from the indictment is representative of the public's – and hence potential offenders' – decreased likelihood of contemplating and being deterred by the bare indictment. Analysis of the APT40 case study shows that civil naming-and-shaming is a suboptimal deterrent measure, especially when compared to the criminal naming-and-shaming of a publicized bare indictment's attack to face.

///

4.8. Summary of Chapter 4 Case Studies; Evidence for Hypotheses

The case studies presented in this chapter have demonstrated the core aspects of the theory on bare indictments. In providing evidence that aligns with predictions, these case studies give proof for the hypotheses.

The PLA Unit 61398 case provided strong evidence for **H1**, **H4**, and **H5**. The timing of the dramatic decline in Chinese cyberattacking activity demonstrated that the bare indictment was the cause of these deterrent effects against prestige-seeking actors; moreover, I ruled out competing explanations that pointed to other events that could have had a deterrent effect. The *respondeat superior* principle led to the prediction that the state would respond to accusations of criminality that were clearly imputable against it; this explained why the Chinese government responded at all even though the Chinese state as an entity was not a named defendant. The discussion of the distinction between criminal and civil naming-and-shaming revealed the nature of the attack to face, therefore supporting both **H1** and **H5**.

Support for **H2** came in the Lazarus case study. As predicted, profit-seeking motives remained undeterred by bare indictment. **H3**, the hypothesis on thrill-seeking motives, was proven by the examination of the SamSam Ransomware cyberattacks coming to an abrupt stop after a bare indictment was publicized.

Proof of **H6** – the hypothesized shift toward profit-seeking – came in Section 4.5.'s analysis of a trend toward profit-seeking motives among Chinese cyberattackers over time; as predicted, § 1030 bare indictments came to be issued almost exclusively against cyberattacks motivated by profit-seeking. In Section 4.6., the discussion of Iranian

cyberattackers further supported **H6** not only by demonstrating a similar trend, but also by providing an empirical example to support **H6**'s theoretical foundation of motive-shifting in a given cyberattacker over time. Finally, the APT40 case study in Section 4.7. once again called to light the distinction between criminal and civil naming-and-shaming, supporting **H1** and **H5** by showing that it is the accusation of *criminal* misconduct that indicted individuals and their nation-states consider to be an attack to face. I provide further evidence for **H5** by looking to Russian case studies in Chapter 5.

CHAPTER 5

IMPUTATION OF SUPERIOR RESPONSIBILITY AND DENIAL OF NATIONAL STATUS: WHY BARE INDICTMENTS CAN DETER NATION-STATES

5.0. Chapter Overview: International Cyberattacks from Russia

To further discuss why nation-states against whose nationals a bare indictment is issued and publicized may see the bare indictment as an attack to national status even when the accused cyberattackers are non-state actors whose motives and objectives are not attributable to the nation-state, this chapter focuses on 18 U.S.C. § 1030 bare indictments issued against Russian state actors and Russian non-state actors.

For two reasons, the Russian cases present a great challenge to the theory on bare indictments. First, the motives of those individuals accused of perpetrating cyberattacks on behalf of the Russian state are not as easily categorized in the framework of status-seeking, profit-seeking, or thrill-seeking. Unlike the cyberattack-enabled espionage operations alleged to be committed by foreign agents of China or of Iran, the cyber-enabled espionage operations allegedly executed by indicted Russian intelligence officers do not primarily appear to take data, but rather to create and disseminate it, with the aim of destabilizing and causing confusion through apparently state-backed "disinformation" campaigns against the U.S. Second, bare indictments do not seem to have achieved specific deterrence against Russian state cyberattackers; because bare indictments have not achieved specific deterrence against these state actors, it appears that they are in turn unlikely to achieve general deterrence against Russian cyberattackers.

Despite these seemingly unfavorable conditions for deterrence, I trace the Russian state's response to Russian non-state cyberattackers to show why the issuance and publicization of bare indictments nonetheless move the ball forward on deterring cyberattacks perpetrated by Russian nationals. First, I briefly review four 18 U.S.C. § 1030 bare indictments issued against individuals alleged to be agents of the Russian state. I analyze the objectives of these arguably state-sponsored cyberattackers to show why their motives – analogous to mixed dominance-seeking and profit-seeking – explain the result that they have been undeterred by bare indictment. Next, I posit that the key to understanding why bare indictments nevertheless exert deterrent influence against the Russian state lies in examining the many bare indictments that have been issued against profit-seeking Russian non-state actors.

In particular, I focus on the case of convicted cyberattacker Roman Seleznev, who was apprehended in a country that has no bilateral extradition treaty with the U.S., to show that the risk of arrest can still achieve specific deterrence against indicted Russian individuals even when the probability of arrest as a result of bare indictment seems to be infinitesimal. I show that, as with the Arrow Tech case in Chapter 6, bare indictments can achieve deterrence because they do not necessarily remain "bare." The Seleznev case, however, sends an even stronger deterrent message than the Arrow Tech case because Seleznev was apprehended in a non-extradition country; it was even more surprising to him, to the Russian state, and to international observers that the bare indictment issued against him would have led to his arrest.

I argue that the arrests and convictions of Russian non-state actors may suggest why counterintelligence officers from Russia's Federal Service of Security (Федеральная служба безопасности; "FSB"), a Russian governmental agency, arrested the Colonial Pipeline cyberattackers, who had been physically located in Russia: attribution theory predicts that the Russian state wanted to visibly distance themselves from these non-state cyberattackers such that the condition necessary for the *respondeat superior* principle would no longer be present. If responsibility – even attenuated responsibility – were to be imputed against Russia for the prolific cyberattacking behavior of its convicted nationals, then the imputed label of criminality would serve as an attack to face that does not deny the non-state cyberattackers' profit-seeking objectives yet does put the Russian state's national status at risk.

5.1. Bare Indictments against Russian State Actors Do Not Deter Disinformation Campaigns

Prior to Russia's February 2022 invasion of Ukraine, the U.S. had issued and publicized four 18 U.S.C. § 1030 bare indictments against Russian state actors. In accordance with attribution theory and Healey's spectrum of nation-state responsibility, these accused cyberattackers can be categorized as Russian state actors because their respective indictments allege that they were officers of, or otherwise carrying out their cyberattacks on behalf of, Russian governmental agencies. The first bare indictment, which was filed on February 28, 2017 and publicly announced on March 15, 2017, alleged a Russian FSB-backed plot to take data from the email provider Yahoo (*Dokuchaev* indictment, line item 1; line item 20); the DOJ alleged that the four charged individuals –

two FSB officers, a third Russian national, and a Canadian national – conspired to "gain unauthorized access to valuable non-public information in individual Yahoo user accounts" for the benefit of the Russian state and sometimes for their "personal financial gain" (DOJ OPA, March 15, 2017). Given the generalized nature of this data theft and the further monetization of the stolen data, it seems clear that the cyberattacks described in this first bare indictment against Russian state actors were primarily motivated by profit-seeking.

The motivations for the next three bare indictments, however, are not so easily categorizable. A comparison to previous case studies illustrates the point. Unlike many other cyberattacks, such as the cyberattacks outlined in the preceding paragraph and several of the cyberattacks described in the previous chapter, these cyberattacks' ultimate aim was not to take data. The indicted Russian state actors' ultimate aim was also not to cause damage to computer systems. Like the mixed profit-seeking and prestige-seeking cyberattacks allegedly carried out as part of Iranian espionage operations, the cyberattacks described in these next three indictments seem to be instrumental in espionage operations. However, the cyberattackers' ultimate objectives were not to take information, but rather to create and disseminate it; in the cyberattacks described in the next three bare indictments, the alleged Russian agents sought to gain unauthorized access to computer systems in order to support "disinformation" campaigns wherein, as alleged in the indictments, they would deliberately spread misleading or false information. As behavioral analysis of motive shows that these disinformation campaigns can be characterized as a mix of profit-seeking and dominance-seeking behavior, the inclusion of a profit-seeking component means that bare indictment is not predicted to deter these indicted Russian state actors.

The first of these disinformation campaigns is described in an indictment filed on July 13, 2018 and publicly announced by the DOJ on the same day. This bare indictment alleged that twelve officers of the Russian Main Intelligence Directorate ("GRU"), a Russian governmental "military intelligence agency" (*Netyksho* indictment, line item 1), had conspired to gain unauthorized access to the "Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of [Democratic candidate] Hillary Clinton" (DOJ OPA, July 13, 2018). The indictment alleges that, after taking documents and messages from these Democratic persons, the Russian GRU officers would then use fictitious names to "stage releases of the stolen documents to interfere with the 2016 U.S. presidential election" (*Netyksho* indictment, line item 20). Because these cyberattacks sought to take wide-ranging caches of data, the cyberattacks were motivated by profit-seeking. Since it is alleged that the cyberattackers sought to use this confidential digital information in order to undermine the U.S. election, the cyberattacks were also motivated by dominance-seeking.

The second disinformation campaign is described in an indictment filed on October 03, 2018 and publicly announced the next day, October 04, 2018, by a DOJ press conference and accompanying press release. This bare indictment charged seven Russian GRU officers – three of whom had also been indicted in connection with the cyberattacks against the Democratic persons – with having violated 18 U.S.C. § 1030 by waging cyberattacks against national and international anti-doping sports organizations, whose information the GRU officers then leaked to "undermine the legitimate interests of the victims, further Russian interests, retaliate against Russia's detractors and sway public opinion in Russia's favor" (*Morenets* indictment, line item 3). The allegations on undermining the international

sports organizations and elevating Russia's position suggest that the cyberattacks against the anti-doping sports organizations were partially motivated by dominance-seeking. However, to accomplish these dominance-seeking activities, the cyberattackers were indiscriminately taking wide-ranging data that could then be sifted through to determine what information would further the activities; this indicates profit-seeking in addition to dominance-seeking.

On October 15, 2020, another bare indictment was issued against six GRU officers, one of whom had also been indicted for the cyberattacks against the Democratic persons. The widespread global cyberattacks alleged included profit-seeking ransomware schemes and "hack-and-leak" disinformation campaigns. The indictment, which was appended to the DOJ's October 19, 2020 press release announcing the indictment, alleged that these GRU officers were members of a GRU cyberattacking group colloquially known in the cybersecurity community as "Sandworm" (*Andrienko* indictment, line item 1).

As evidenced by the U.S. government's need to turn to alternate policy means other than bare indictment, Russian state cyberattackers such as Sandworm have been undeterred by bare indictment. In late April 2022, the U.S. Department of State announced a bounty of up to ten million USD for "information leading to the identification or location of any" indicted member of Sandworm (U.S. Department of State 2022; Whittaker 2022). At around the same time, the private computer company Microsoft released a report technically attributing Sandworm as a perpetrator of "hybrid" warfare cyberattacks amidst Russia's military invasion of Ukraine (Microsoft Digital Security Unit, 2022). Although Sandworm's and other Russian state cyberattackers' objectives are not cleanly

categorizable as purely profit-seeking, the inclusion of a profit-seeking component in the cyberattacks that seek to sustain disinformation campaigns means that they are unlikely to be deterred by bare indictment; the package of informal sanctions neither directly denies nor indirectly outweighs profit-seeking objectives. As has been discussed, the expected benefit of profit can be so high that it enables the presence of other objectives such as dominance.

Extrapolating from the theory on bare indictments provides another way of explaining why Sandworm remains undeterred. The reason why bare indictments do not tend to deter profit-seeking actors is that, unlike how the package of informal sanctions directly denies the expected benefit of status and tends to outweigh the expected benefit of emotional thrill, the expected cost of informal sanctions is usually not enough to outweigh the expected benefit of economic profit. Analogously, if the expected benefit is "the success of a state-backed disinformation campaign," the shaming measures and practical consequences imposed by informal sanctions are unlikely to be enough to outweigh Sandworm's expected benefit. Indeed, Andy Greenberg in *Wired* reports that a cybersecurity policy practitioner has observed that the Russian state seems to be less sensitive to shaming measures than is the Chinese state: "Naming and indicting individual culprits, as the US Justice Department did with Chinese hackers in 2014, may not be the right approach to Russia... 'The Russians are less affected by shame,' [cybersecurity policy practitioner Laura Galante] says. 'The Chinese felt incredibly demeaned by what happened with the indictment and that made it powerful'" (Greenberg 2016).

5.2. Bare Indictments Enable Apprehension and Conviction of Russian Non-State Cyberattackers

Despite Russia's diminished sensitivity to attacks on status, looking to the Russian state's responses to bare indictments issued against Russian non-state cyberattackers shows that it would be a mistake to dismiss bare indictment as a futile move against a Russian state impervious to shaming measures. The indictment of Russian non-state actors seems to have embarrassed the Russian state; I suggest that three factors may have contributed to the expected cost of the Russian state such that it, in accordance with attribution theory, subsequently cooperated with the U.S. government in apprehending Russian non-state actors. First, the number of Russian non-state actors indicted under 18 U.S.C. § 1030 is – relatively speaking – extremely high. The FDD CCTI dataset (Logan and Patel 2020a) includes at least fifteen 18 U.S.C. § 1030 indictments that could arguably be characterized as having been issued against Russian nationals who are non-state actors. The approximately fifteen 18 U.S.C. § 1030 indictments issued prior to early 2020 against Russian non-state actors alone well exceed the respective number of 18 U.S.C. § 1030 indictments issued against nationals of any other foreign country. On the FDD CCTI dataset, there are only seven 18 U.S.C. § 1030 indictments issued against Chinese nationals, whether state actors or non-state actors. This is less than half the number of 18 U.S.C. § 1030 indictments issued against Russian non-state actors alone. The number of 18 U.S.C. § 1030 indictments issued against Iranian nationals is even fewer, at only six. Since each bare indictment brings with it a new opportunity for publicization of Russian cybercriminal activity, the sheer number of indictments could be embarrassing to the Russian state.

Second, the indictments were issued against Russian non-state actors who were primarily profit-seeking. Although the theory on bare indictments predicts that profit-seeking actors are least likely to be specifically deterred by bare indictment, bare indictments here sent a deterrent message because bare indictments' result in imposition of formal legal consequences was enough to outweigh even profit-seeking objectives. For further discussion of why actual apprehension also contributes to bare indictments' deterrent effect irrespective of motive, see Chapter 6.

Third, then, is that these seemingly "bare" indictments have often led not only to arrests, but also convictions. The U.S. government's public announcement of this information means that this information can serve as a deterrent message to the Russian state and to global audiences. Russian national Vladimir Zdorovenin, the father in a father-and-son cyberattacking team, was indicted under 18 U.S.C. § 1030 in May 2007 (USAO SDNY, January 04, 2013). Zdorovenin was arrested in Switzerland on March 27, 2011 and was extradited to the U.S. in January 2012 (USAO SDNY, January 17, 2012). In February 2012, he pled guilty to related charges; on January 04, 2013, he was sentenced to prison time (USAO SDNY, January 04, 2013). Nikita Vladimirovich Kuzmin, a Russian national who was only seventeen years old when he began mounting cyberattacks in 2005, was arrested in November 2010 (Zetter 2013). Kuzmin pled guilty to charges listed in a 2013 indictment (USAO SDNY, May 02, 2016). The information from a USAO SDNY press release detailing Kuzmin's sentencing indicates that his cyberattacks were profit-seeking given that Kuzmin further monetized his malware, known as Gozi: "Unlike many cybercriminals at the time, who profited from malware solely by using it to steal money, KUZMIN rented out Gozi to other criminals, pioneering the model of cybercriminals as service providers for other

criminals... KUZMIN made at least a quarter of a million dollars renting and selling Gozi to other criminals" (USAO SDNY, May 02, 2016). Dmitry Belorossov, who according to his lawyer "was only a teenager" when he used the Citadel malware to "gain access to more than 7,000 computers" as a member of a crime ring that took "online banking credentials for U.S.-based financial institutions, credit card information, and other personally identifying information," was extradited to the U.S. from Spain in 2014 (Ax 2015). In July of that year, Belorossov pled guilty to violations of 18 U.S.C. § 1030; he was sentenced to prison time and was required to pay $322,409.09 of restitution (USAO Northern District of Georgia 2015). Not only were indicted Russian cyberattackers extradited, but they could also be apprehended if they were physically located within the U.S. itself, as was the case for convicted Los Angeles-based Russian cyberattacker Mikhail Konstantinov Malykhin (USAO Central District of California 2018). In total, research shows that thirteen indicted Russian nationals across twelve of the fifteen indictments were arrested, convicted, and sentenced to formal legal consequences including prison time and monetary fines.

5.3.0. Bare Indictments Lead to Arrests in Non-Extradition Jurisdictions [RNOST-06]

Among these cases in which seemingly bare indictments of Russian nationals led to the individuals' apprehension and conviction, the case of Roman Valeryevich Seleznev stands out for further study; because it was highly improbable that Seleznev would be apprehended, his arrest and conviction sends a strong deterrent message to future potential offenders. Chapter 4's Chinese case study of Su Bin's arrest and guilty plea, and Chapter 6's Iranian case study of the cyberattackers who were specifically deterred by their

co-conspirator's arrest, demonstrate that bare indictments do not necessarily remain "bare." Those two cases show that if indicted individuals are physically located in a country that has an extradition treaty with the U.S., they can be arrested and extradited to the U.S. to face trial. The Seleznev case, however, sent a message that indicted cyberattackers who are foreign nationals would face the risk of arrest and extradition even when visiting jurisdictions that had *no* extradition treaty with the U.S. Because the Seleznev case communicates to cyber adversaries that the highly improbable is a real risk, it shows that bare indictments can deter because informal sanctions include practical consequences that raise the potential offender's expected probability of cost, with the cost here being the subsequent imposition of formal legal consequences.

5.3.1. A Family Vacation Leads to A Wealthy, Well-Connected Russian Cyberattacker's Arrest

Roman Valeryevich Seleznev, against whom an 18 U.S.C. § 1030 indictment had been issued under seal in March 2011, is described in news reports as the son of a member of the Russian parliament (Bertrand 2015; Walker 2014). Seleznev, a Russian non-state cyberattacker, was apparently motivated by profit-seeking. A DOJ OPA press release describing his guilty plea and sentencing states that Seleznev admitted to using unauthorized access to take victims' credit card numbers, causing losses of tens of millions of dollars (DOJ OPA, November 30, 2017). It could also be argued that Seleznev was primarily thrill-seeking or prestige-seeking, since details indicate that Seleznev often enjoyed flaunting his symbols of wealth; seized photographs from his electronic devices show him posing with boats, with stacks of paper currency, and with sports cars all

apparently belonging to him or otherwise in his possession (Bertrand 2015). However, Seleznev seemed to recognize that a lifestyle comprising these symbols of wealth needed to be sustained by actual monetary profit; Seleznev further monetized the taken data by setting up an online marketplace and selling the credit card numbers he had stolen (DOJ OPA, November 30, 2017). Moreover, unlike the SamSam Ransomware cyberattackers who victimized sympathy-inducing targets such as healthcare providers, reports indicate that Seleznev mostly took credit card numbers by cyberattacking "restaurants and small businesses" (Walker 2014); since small businesses usually gather customers' credit card information in one digital location, cyberattacking centralized targets was an efficient means of gathering as many credit card numbers as possible from each cyberattack. Considering that he optimized his cyberattacks, took credit card numbers, and further monetized the data he took, convicted Russian non-state cyberattacker Seleznev is best categorized as a primarily profit-seeking actor.

On Monday, July 07, 2014, the U.S. Department of Homeland Security ("DHS") announced that Seleznev had been arrested by the U.S. Secret Service at the start of the weekend two days prior (DHS 2014). In subsequent news reports, it later emerged that he had been apprehended in the Maldives, a nation that does not have an extradition treaty with the U.S. Computer security reporter Brian Krebs states that Seleznev had reportedly been vacationing at a Maldivian luxury resort (Krebs 2017); there, Seleznev spent approximately twenty thousand USD on accommodations during what other news reports described as a "family vacation" (Bertrand 2015; Solis 2019). According to Krebs, the indicted Seleznev's apprehension in the Maldives was startling to international observers, and especially so to Russian nationals, because the Maldives had a reputation as a safe

haven for wealthy Russian vacationers (Krebs 2019). For point of reference, an early 2022 travel article from an online culture magazine describes the Maldives as a favored travel destination of Russian oligarchs (Rogers 2022). Even today, the Maldives is seen as – quite literally – a safe harbor for wealthy Russian nationals. Amidst the Russian invasion of Ukraine beginning in February 2022, the Maldives has been the subject of controversy for reportedly sheltering the multimillion-dollar yachts of Russian oligarchs whose property – yachts included – had been subject to U.S. economic sanctions (Pal and Junayd 2022). As a wealthy Russian national vacationing in the Maldives, Seleznev himself was shocked by his apprehension under the U.S. bare indictment; Krebs quotes a report that upon Seleznev's apprehension, Seleznev immediately exclaimed in disbelief that the U.S. has no extradition treaty with the Maldives (2019).

Because the U.S. has no extradition treaty with the Maldives, Seleznev's arrest – while legally licit – is also surprising from a legal standpoint. Upon Seleznev's appeal, the Ninth Circuit upheld Seleznev's apprehension, writing "Because there is no extradition treaty between the United States and the Maldives, U.S. agents did not violate an extradition treaty" (*Seleznev* memorandum, 2). However, in the absence of an extradition treaty with the U.S., the Maldivian authorities had no legal obligation to cooperate with the U.S. agents. Why, then, did the Maldives cooperate with Seleznev's apprehension? Looking to the reported details of Seleznev's apprehension provides a clue as to the legal framework that may have been leveraged to facilitate international cooperation: the Customs Mutual Assistance Agreement ("CMAA") between the U.S. and the Maldives.

5.3.2. U.S.-Maldives CMAA Facilitated Arrest in Non-Extradition Country

Before explaining how the U.S.-Maldives CMAA was likely instrumental in Seleznev's apprehension, I first address an alternate possibility. A 2015 report from *Business Insider* summarizes a *Bloomberg* article in reporting that the "Secret Service… solicited the help of the Maldivian police superintendent (with whom the [U.S.] State Department has a close relationship) in capturing Seleznev" (Bertrand 2015). Irrespective of whether or not this is true, it still leaves questions as to why – as the *Business Insider* article suggests in the very next sentence – the Maldivian law enforcement authority that detected and detained Seleznev can be inferred to be the Maldivian Customs Service (Bertrand 2015), rather than the Maldivian police force.

Like a Mutual Legal Assistance Treaty ("MLAT"), a CMAA's purpose is to provide a legal framework to facilitate information-sharing between the respective law enforcement authorities of the nation-states that are the parties to the agreement (MacCormack 2009, 464, at footnote 96; U.S. Customs and Border Protection 2021). The difference between a MLAT and a CMAA is that an MLAT's framework usually covers all law enforcement agencies of the respective nation-states, whereas a CMAA's framework extends only to the Customs agencies of the respective nation-states. The U.S.-Maldives CMAA became legally binding as of June 25, 2005. Under broad conditions – essentially, whenever a matter relating to Customs' purview is invoked – the terms of the U.S.-Maldives CMAA create a legal obligation for the respective Customs authorities of the U.S. and the Maldives to cooperate with each other by rendering assistance to one another and sharing information with each other. The CMAA not only obligates each party to cooperate upon request of the other party, but also encourages the respective Customs authorities to share information

"on their own initiative" when the Customs authority of one party believes that such information may be useful to the Customs authority of the other party (Article IV, Section 3.).

In particular, I would identify two provisions of the U.S.-Maldives CMAA that could have facilitated Seleznev's arrest. One of these provisions is Article IV, Section 3: "In situations that could involve *substantial damage* to the economy, public health, public security, or *similar vital interest* of the other Party, the Customs Administrations, wherever possible, *shall supply such information without being requested to do so* [emphases added]." The ending clause's use of the word "shall" rather than opposed to "should" or "may" creates a legal obligation to cooperate when the provision is invoked. In accordance with this provision, to invoke the legal obligation to cooperate, U.S. Customs would only have had to communicate to the Maldivian Customs Service that – as evidenced by the indictment – the U.S. had reason to believe that Seleznev's cyberattacks had been responsible for tens of millions' of USD worth of damage to U.S. nationals, and that – as evidenced by Seleznev's ostentatious profit-seeking behavior – the U.S. had reason to believe that Seleznev would continue his damaging cyberattacks. Article IV, Section 3 is the more efficient provision for the U.S. to utilize. Under Article VII, Section 1, any "request" under the U.S.-Maldives CMAA must be made in writing. Since Article IV, Section 3 expressly states that this route of cooperation does not require "being requested," the U.S.'s communication under Article VII, Section 3 does not have to be in writing and is therefore likely to be the more efficient, less time-consuming way to secure cooperation.

A second provision that the U.S. could have invoked was Article IV, Section 2(a)-(c), on requests for "special surveillance." Subsections (a) through (c) of this provision, regarding the objects of the surveillance, are broadly drawn; arguments could straightforwardly be made that Seleznev or his possessions qualify for surveillance by the Maldivian Customs Service. However, pursuant to this provision, invoking the legal obligation to cooperate by conducting "special surveillance" requires a written "request." Article VII provides hints as to why making a written request is generally less efficient than making an oral request. Written requests are generally more time-consuming to prepare than are oral requests. This is especially true when written requests must comply by the parameters called for by Article VII, Section 2, subsections (a)-(e). As evidenced by the special alternate protocol for "urgent situations" (Article VII, Section 1), it usually also takes longer to secure official approval for a written request than for an oral request. By the time a written request had been prepared, sent, and approved, Seleznev could long have fled the Maldives.

This analysis shows that even without a friendly "close relationship" with a high-ranking member of foreign law enforcement, a CMAA can be leveraged to aid in apprehension of indicted foreign nationals who travel into and out of jurisdictions that have no bilateral extradition treaty with the U.S., as traveling into and out of these jurisdictions will put the indicted foreign nationals within the purview of the jurisdiction's Customs authorities. For this reason, being arrested in a country that does not have an extradition treaty with the U.S. becomes a contemplable risk, which can further enhance the deterrent effect of seemingly "bare" indictments that are issued.

5.3.3. Possibility of Arrest in Non-Extradition Countries Enhances Deterrence

The Seleznev case sends the deterrent message that indicted Russian cyberattackers – even those who were wealthy and politically connected – could be apprehended even in jurisdictions thought to be friendly toward Russian nationals. Evidently, the publicization of Seleznev's apprehension in the Maldives meant that the deterrent message of this bare indictment was transmitted to the Russian state. Member of Russian Parliament Valery Seleznev, the father of Roman Valeryevich Seleznev, first denied that Roman Seleznev was his son (Walker 2014). A news report published on July 08, 2014 – the day after the DHS's announcement of Roman Seleznev's arrest – states that the elder Seleznev had made the implausible assertion that "his son did not have any knowledge of computers" (Walker 2014). Later, the elder Seleznev indignantly described the allegations as a "monstrous lie" (Walker 2014). The Russian foreign ministry immediately condemned Seleznev's arrest, characterizing it as a "kidnapping" (Walker 2014, Bertrand 2015).

With Seleznev's arrest in the Maldives having been made known to the Russian state, the Seleznev case would tend to deter indicted Russian nationals from traveling outside Russia at all. In turn, this restriction on travel can deter Russian nationals from committing cyberattacks. Hinck and Maurer (2020) describe the international community's outrage at learning that, in April 2018, Dutch authorities had deliberately decided not to arrest four GRU officers when there was ample evidence to indicate that the four GRU officers had flown into Amsterdam and driven to The Hague to mount a cyberattack against the computer systems of the Organisation for the Prohibition of

Chemical Weapons ("OPCW") (Hinck and Maurer 2020, 544-545; Rosenberg 2018). Hinck and Maurer call attention to the fact that, as of April 2018, no bare indictment had yet been issued against these four GRU officers (2020, 544-545).

Recall that the anti-doping case study discussed in a preceding section of this paper involved a bare indictment that was issued against seven Russian GRU officers, three of whom had also been indicted in connection with the cyberattacks against the Democratic persons. The other four GRU officers were the very same four who had traveled to the Netherlands in April 2018. As this shows, the ability to travel to foreign jurisdictions without being apprehended can be crucial for state-sponsored cyberattackers; notwithstanding the increasing ability to mount cyberattacks remotely, cyberattacks like the one the later-indicted GRU officers allegedly attempted against the OPCW can be facilitated by physical proximity. Had a bare indictment against these four GRU officers been issued and publicly announced before they were to travel to the Netherlands, the bare indictment would have solidified the risk of their arrest, deterring them from allegedly mounting the cyberattack against the OPCW. Note that apprehension is not merely a disruptive measure, but also a deterrent measure. The risk of arrest would not necessarily have disrupted the apparently attempted cyberattack against the OPCW, as arrest could have occurred after the attempt was already complete. Rather, an increase in the expected probability of apprehension – as communicated by the issuance and public announcement of a bare indictment – could have instilled a fear of the after-the-fact consequences and therefore have deterred those GRU officers from allegedly mounting the OPCW cyberattack.

Even when it seems highly improbable, then, bare indictments carry a risk of arrest and conviction for indicted foreign nationals who are traveling to other jurisdictions. The high conviction rate among Russian nationals subject to § 1030 bare indictment likely enhanced the cumulative effects of the repeated attacks to national status that, as I will argue in the next section, the Russian state contemplated and cooperatively preempted.

5.4.0. Bare Indictments' Role in Prompting Russian Arrest of Colonial Pipeline Cyberattackers

Surprisingly, the Russian state has cooperated with the apprehension of its own nationals even before a § 1030 bare indictment was issued against them. This suggests that the avoidance of bare indictment may have induced the Russian state's diplomatic cooperation, notwithstanding that it was not legally obligated to do so, with the U.S.; by convincing the Russian state to take action, the avoidance of bare indictment may have hence enhanced the deterrence of Russian non-state cyberattackers. The previous section shows that bare indictments have exerted pressure on the Russian state. As evidenced by the indignant responses of the Russian government ministry, the Russian state may not be as sensitive to prestige as is the Chinese state, but Russia can still be embarrassed by bare indictment. Bare indictments impose a contemplable risk of arrest, ergo a contemplable risk of criminal conviction, ergo a contemplable risk that – no matter how "bare" the indictment may initially seem – formal legal consequences may be imposed. The Seleznev case strengthened the general deterrent force of bare indictment by showing that a wealthy, politically connected Russian national was arrested and convicted. An underlying reason that bare indictments can deter cyberattackers is because bare indictments impose

a contemplable risk of formal legal consequences; this risk has been especially borne out against indicted Russian cyberattackers.

Given that the 18 U.S.C. § 1030 bare indictments that have led to arrests and convictions of Russian nationals – subsequently embarrassing the Russian state – have overwhelmingly been issued against non-state actors, attribution theory would predict that the Russian state would be inclined to take action that distances itself from any future non-state Russian cyberattackers. Recall that Hamilton (1986) writes that supervisory oversight can lead to responsibility attribution for the actions of subordinates: "Authorities may be held responsible, legally or morally, as a function of expectations attached to their role rather than causality per se: What they *should have* done, seen to, or prevented, rather than anything they actually did [emphasis in original]" (120). Like *respondeat superior* for legal liability, attribution theory predicts that responsibility and blame for misconduct will fall on a superior when it is perceived that the superior could and should have done something to prevent the misconduct. This can be analogized to the situation of the Russian state. Just as a supervisor that fails to prevent subordinates from work-related misconduct may be held both legally and morally responsible, a state that cannot prevent its own nationals from running rampant in committing criminal cyberattacks is likely to be seen – by other members of the international community, or even by itself – as dysfunctional. Moreover, as has been discussed in Chapter 2 and as will be further discussed in Chapter 8, administering the criminal law is seen by classical CDT as the constitutive function of statehood; failure to administer the criminal law could contribute to the perception or self-perception of nation-state incompetence. Any person who holds the perception that the Russian state could and should have done something to curb

Russian non-state cyberattacks – even if said 'person' is the Russian state itself – is more likely to attribute responsibility for Russian non-state cyberattacks to the Russian state. Thus, the principles of attribution theory yield a prediction that the Russian state, in order to avoid responsibility – whether legal, moral, diplomatic, or otherwise – for Russian non-state cyberattacks being attributed to it in its capacity as a state, would be incentivized to 'crack down' on cyberattacks committed by its nationals who are non-state actors. This condemnatory action would suggest that the Russian non-state cyberattacks did not occur under the imprimatur of the Russian state, and would indicate that the Russian state is taking "corrective action" (Solis 2010, 381) to curb the cyberattacks such that the *respondeat superior* condition would not apply.

5.4.1. The Colonial Pipeline Cyberattack [RNOST-21]

The predictions of attribution theory suggest a reason why Russia cooperated with the U.S. in arresting the suspected non-state Colonial Pipeline cyberattackers. On May 07, 2021, cyberattackers gained unauthorized access to the computer systems of Colonial Pipeline, a natural gas company that supplies fuel to the southern United States as well as the East Coast of the United States (Kerner 2022). The cyberattackers infected Colonial Pipeline's computer systems with ransomware, rendering those computer systems inaccessible to authorized users. Consequently, Colonial Pipeline's operations were brought to a standstill. During the five days that Colonial Pipeline was shut down, there were gas shortages across the East Coast and the southern United States (Knutson 2021). It is also likely that the news of the cyberattack aggravated these gas shortages by causing

so-called "panic buying" (Rapier 2021). Not knowing how long the gas shortages would last, consumers nationwide queued at fuel stations to purchase gas for their cars (Romo 2021). While recovering from the ransomware attack, Colonial Pipeline's operations did not restart until May 12, 2021 (Kerner 2022).

The cyberattack against Colonial Pipeline was swiftly technically attributed to a Russian profit-seeking actor. On May 10, 2021, the U.S. Federal Bureau of Investigation ("FBI") released a brief, two-sentence-long public statement confirming that DarkSide ransomware had been used to execute the Colonial Pipeline cyberattack (FBI 2021). An analysis from *NBC News* explained that DarkSide ransomware was "believed to be operated by a Russian cybercrime gang referred to by the same name," DarkSide (Collier 2021). Cybersecurity analysts speculated that the DarkSide gang's actions must have been condoned by the Russian state, since the Russian government seemed to give the DarkSide gang free rein to carry out international cyberattacks (Carmack 2021; see also Whitney 2021; Shinkman, May 11, 2021). On May 11, 2021, Russian government spokesperson Dmitry Peskov denied that the Russian state had played any part in executing the Colonial Pipeline cyberattacks (Shinkman, May 11, 2021), but Peskov did not seem to deny the contention that the Russian state had created an environment that allowed DarkSide to carry out international cyberattacks.

Looking to DarkSide's target, as well as to DarkSide's own statements, shows that these apparently non-state actors were primarily motivated by profit-seeking. Technology analysis contributor Charlie Osborne wrote that the gas shortages and widespread panic seemed to be only a byproduct of the DarkSide cyberattackers' main goal: "It should be

noted that DarkSide operators targeted the business side rather than operational systems, which implies the intent was money-orientated rather than designed to send the pipeline crashing down" (Osborne, May 13, 2021). Furthermore, DarkSide itself released a statement claiming to be "apolitical"; despite the chaos caused by DarkSide's cyberattack of Colonial Pipeline, DarkSide purported, "Our goal is to make money" from DarkSide's ransomware (Osborne, May 14, 2021).

The Colonial Pipeline cyberattack became an international issue between the American state and the Russian state. In reporter Joseph Marks' May 06, 2022 retrospective of the Colonial Pipeline cyberattack, Marks characterized the cyberattack as "a seismic shift in which a cyberattack had real-world implications for tens of thousands of average Americans who spent hours in gas lines" and called attention to the fact that it had "prompted a diplomatic confrontation between [U.S.] President Biden and Russian President Vladimir Putin during a Geneva Summit. Biden demanded that Putin prevent Russia-based cybercriminals from targeting U.S. critical infrastructure including pipelines, energy and financial firms" (Marks 2022). According to Marks, this "diplomatic confrontation" occurred on June 16, 2021 (Marks 2022).

On November 08, 2021, the DOJ OPA announced a § 1030 bare indictment against an alleged member of REvil, which is a cyberattacking group that is related to the DarkSide group (Greig 2022); however, this bare indictment and associated recovery of ransom money concerned ransomware cyberattacks that took place in August 2019 (DOJ OPA, November 08, 2021; *Polyanin* indictment, 16-17), which is prior to the May 2021 Colonial Pipeline cyberattack. As of the time of this writing, research has not yielded anything to

indicate that the alleged member of REvil has been apprehended; the bare indictment against this apparently profit-seeking Russian non-state actor remains bare.

Despite that the FBI had technically attributed the Colonial Pipeline cyberattack to Russian non-state actors, no 18 U.S.C. § 1030 bare indictment has been publicly announced against DarkSide's members for the Colonial Pipeline cyberattack either prior to or following diplomatic communication between Biden and Putin at the Geneva Summit on June 16, 2021.

5.4.2. Russia Arrested Its Own Nationals to Recover Its National Status

In January 2022, approximately six months after the Geneva Summit, came the surprising news that the Russian FSB had taken action in arresting fourteen of Russia's own nationals who were suspected cyberattackers; as highlighted by the U.S., Russian law enforcement had confirmed that among these suspected cyberattackers was an individual to which the Colonial Pipeline cyberattack had been technically attributed. On January 14, 2022, a Biden administration official and the FSB each confirmed the arrests (Miller 2022). Maggie Miller wrote in *Politico* that the arrests of these Russian nationals were the product of the diplomatic negotiations between the U.S. and Russia: "The arrests followed months of negotiations between the Biden administration and Russian officials" (Miller 2022). According to *CNN*, the Russian government stated that the fourteen arrested individuals would not be extradited; rather, Russia – without providing further details – assured that the individuals would be prosecuted under Russia's domestic justice system (Lyngaas 2022).

Attribution theory explains why the avoidance of bare indictment likely contributed to the Russian state's decision to arrest its own nationals and prosecute them under Russian law rather than extradite them. While avoidance of bare indictment does not preclude other factors in the negotiation process from also contributing to Russia's decision, the explanation yielded by looking to the principles of attribution theory and the role of bare indictments holds up well to competing explanations.

For instance, some analysts have raised the possibility that Russia wanted to signal that it was cooperating because Russia was attempting to sway U.S. opinion in its favor so that the U.S. would be less likely to impose economic sanctions or other diplomatic costs upon Russia if it were to invade Ukraine (see Miller 2022; Lyngaas 2022; Greig 2022; Chalfant 2022). As of January 2022, there were already indicia that Russia was preparing for a military invasion of Ukraine. Miller, for instance, notes that the arrests occurred amidst "rising tensions between the U.S. and Moscow over a Russian troop buildup on the Ukrainian border" (2022). Moreover, the hybrid warfare cyberattacks suspected to be waged by the Russian state against Ukrainian government websites had already begun (Chalfant 2022). The explanation of avoiding bare indictment, however, harmonizes with these alternative explanations. The Seleznev case study established that the Russian state had been embarrassed by bare indictment, and therefore would likely anticipate that it would continue to be embarrassed if further bare indictments against profit-seeking Russian non-state cyberattackers were imposed. If the Russian state had been solely motivated by wanting to sway U.S. opinion in its favor ahead of Russia's impending invasion of Ukraine, then the Russian state would not have been so adamant about prosecuting the arrested Russian nationals domestically and excluding U.S. involvement in

the domestic prosecution. It would have demonstrated much more cooperation with the U.S. if Russia had instead collaborated with the U.S. in prosecuting these individuals under Russian law, and it would have been efficient for the Russian prosecutors to draw upon the technical attribution that had – as it seems from the FBI's terse press statement on May 10, 2021 – already been made by the FBI.

Unless Russia was motivated by the avoidance of embarrassment and by attribution theory's prediction of avoiding responsibility, it is unlikely that Russia would have been so adamant about prosecuting the arrested individuals domestically and keeping the U.S. 'out of the loop,' so to speak. Bare indictments, therefore, can serve as a means of embarrassing and hence deterring a state target; they imply that the state target cannot perform the function of preventing its own nationals from committing criminal acts. The issuance of criminal charges by a foreign jurisdiction – the U.S. – is a formalization of attribution theory's principle that responsibility will fall on a superior if it is perceived that the superior, in its role as superior, could and should have prevented the misconduct of a subordinate. Biden had already established this perception through his diplomatic communications with Putin; a bare indictment made common knowledge would further have attacked Russia's status by strengthening this perception among other members of the international community, threatening Russia's face. Since bare indictments had already embarrassed Russia by the implication that it could not keep its own nationals from committing international cyberattacks, Russia was incentivized to counter the perception by showing that it was able to 'do its own job' of overseeing and administering its domestic criminal justice system. Russia's cooperation also made it less likely that the U.S. would issue and publicize a bare indictment in response to the Colonial Pipeline cyberattack that

was apparently perpetrated by a Russian national, so it seems that Russia preemptively cooperated to prevent the U.S. from making another attack on the prestige of the Russian state; avoidance of bare indictment again speaks to Russia's desire to evade embarrassment. Both for the audience of the international community and for the sake of its self-perception, Russia needed to allay imputed responsibility by showing that it *was* taking action to prevent misconduct by its nationals.

A further, more cynical perspective on Russia's option of collaborating with the U.S. on a domestic prosecution under Russian law is that the Russian FSB could have used working with the American FBI not only as a means of establishing friendly relations between these counterpart U.S. and Russian law enforcement authorities, but also as a means of gaining intelligence about the FBI's methods and operations that would have been highly beneficial to the Russian state. Prior to Russia's February 2022 invasion of Ukraine, the prospect of collaboration between U.S. and Russian authorities would not have been as preposterous as it may sound. Recently, Russian and U.S. authorities frequently cooperated in granting hundreds of each other's routine information-sharing requests per year (Finn 2013). Reciprocal collaboration between the U.S. and Russia may not only occur voluntarily, but also when required; as previously alluded to in the Seleznev case study, the CMAA in force between the U.S. and Russia would legally *obligate* the respective Customs authorities of each nation-state to assist one another when broad conditions apply or are invoked (White House 1994, Article 3; White House 1994, Article 4).

Indeed, one particularly high-profile joint investigation both establishes a recent precedent for collaboration between U.S. and Russian authorities and evidences the idea

that collaborative efforts from Russian authorities would have done much more to sway U.S. opinion in the Russian state's favor. The FBI and the FSB collaborated in conducting the high-profile criminal investigation of the 2013 Boston Marathon bombings (Finn 2013, Soldatov and Borogan 2017), and the FSB's successful collaboration with the FBI drew much celebration from U.S. congressmembers and from the U.S. White House (Soldatov and Borogan 2017).

As Russian investigative journalist Andrei Soldatov wrote in an opinion piece for the *Washington Post* on February 01, 2022, Russia's cooperation in the arrest of its own nationals was not an attempt to garner U.S. favor, but rather, an attempt to preserve Russia's rank in the international order: "What we're seeing is less an effort to sow goodwill in the West than an attempt by the FSB to affirm its rising status as the major bureaucratic force behind Russian foreign policy" (Soldatov 2022). Russia had been embarrassed by the cybercriminal activity of its nationals. As those profit-seeking cyberattacks could then be attributable to the state under attribution theory, they threatened the Russian state's status. The *respondeat superior* condition was present for the members of the global order to perceive that either the Russian state was condoning the profit-seeking cybercriminal activity, which would fall around the middle of Healey's spectrum; or the Russian state fell on the low end of Healey's spectrum, which carries the unflattering and status-destroying implication that the Russian state was hopelessly inept at keeping the profit-seeking cybercriminal activity under control. Russia's cooperation in the arrest distanced itself from the non-state cyberattackers, avoiding the non-state cyberattackers' misconduct from reflecting poorly on the Russian state in accordance with attribution theory; in addition to preventing this loss of status, Russia's cooperation in the

arrest further strengthened its prestige by demonstrating the capabilities of its national security service. If demonstrating cooperation to sway U.S. opinion had been Russia's main goal, the Russian state would have made a much stronger demonstration of cooperation – and might have had much more to gain from the opportunity to obtain other valuable U.S. intelligence – if Russia had indicated its willingness to collaborate with the U.S. Instead, Russia's adamance about keeping the U.S. out of its domestic prosecution of the arrested nationals is an indication of Russia's desire to allay responsibility and avoid embarrassment. Attribution theory and *respondeat superior* predict that the criminalization of the profit-seeking Russian nationals was imputable to the Russian state; as a result of the imputation of responsibility, it was not just the non-state cyberattackers' face that the indictments attacked, but also the Russian state's national face.

To avoid another iterative assignment of blame that would result if the Russian state again "took no corrective action upon learning of" the cyberattacking activity that had happened under its oversight (Solis 2010, 381), the Russian state had to demonstrate that it was taking corrective law enforcement action in response to the Colonial Pipeline cyberattack so that Russia would not meet the condition necessary for *respondeat superior* to apply. The indicted and convicted profit-seeking Russian non-state cyberattackers may not have cared much about attacks to face, but it seems that the Russian state did care about bare indictments' repeated attacks on Russian national status.

///

///

5.5. Chapter Conclusion: General Norm-Setting at the Nation-State Level

These case studies of publicized § 1030 bare indictments issued against Russian nationals evidence **H5**, showing that nation-states against whom bare indictments are imputable will be sensitive to the attack on national face that bare indictments achieve. The additive impact of the repeated attacks to face made by numerous accusations of criminality against Russian non-state actors was imputable to the Russian state in accordance with the principle of *respondeat superior.* Because the Russian state – like many other states – can be assumed to care about its national face, it reacted as predicted, by affirming its own federal security forces' capabilities. Thus, bare indictments led to Russia's arresting its own nationals before a bare indictment could be issued against them. Since these arrests were a bid to recover global status rather than an attempt to curry favor with the U.S. government, Russia insisted on handling the suspected cyberattackers' cases domestically rather than jointly, demonstrating that Russia was not incompetent at administering criminal justice.

Russia's willingness to take the unprecedented step of apprehending its own nationals raises the expected risk of apprehension and therefore serves as a further general deterrent for potential cyberattackers, even those who are apparently profit-seeking. Strikingly, bare indictment seems to have achieved these deterrent effects even though the Russian state's level of imputed responsibility was relatively weak, falling at the low end of Healey's spectrum. The implication that Russia was hopelessly incompetent – that in allowing cybercriminal behavior to run rampant it was failing to perform even the minimal functions of statehood, such that the U.S. had to step in to 'do Russia's job' – threatened Russia's national status; bare indictments' attack to face hence led to a general deterrent

effect. This analysis suggests that § 1030 bare indictments should be issued and publicized to achieve general deterrence even when the individuals to be indicted are profit-seeking and therefore unlikely to be specifically deterred. By making common knowledge an accusation of criminality that is then even weakly imputable against the nation-state, bare indictments can prompt a nation-state to intervene in criminal cyberattacking behavior so that the *respondeat superior* condition for imputed responsibility does not apply. In turn, the target nation-state's affirmation that this cyberattacking behavior is criminal and hence unacceptable aids in setting and strengthening global norms that can achieve general deterrence against international cyberattacks, even those that are profit-seeking.

CHAPTER 6

OTHER ASPECTS OF BARE INDICTMENTS:

IMPOSITION OF APPREHENSION RISK AND INTERACTION WITH ECONOMIC SANCTIONS

6.0. Chapter Overview: Other Aspects of Bare Indictments

Going beyond the core of the theory on why bare indictments deter cyberattacks, examining two cases in which the U.S.'s issuance and publicization of a bare indictment under 18 U.S.C. § 1030 led to an unexpected result yields insight on other aspects of bare indictments.

A bare indictment unsealed on April 21, 2016 is demonstrative of a unique deterrent feature: while it may be unlikely that a bare indictment will ever result in an arrest, the issuance of a bare indictment gives cyberattackers a contemplable risk of apprehension. In this Arrow Tech case study, which is discussed in Section 6.2., the evidence on the primary motives of the alleged cyberattackers is ambiguous. Because the motives of the alleged cyberattackers in the Arrow Tech case are unclear, the core theory on bare indictments would not yield a consistent prediction. However, examining the case shows that bare indictments nevertheless deterred through another mechanism that operates irrespective of motive. This alternative deterrent mechanism stems from the fact that "bare" indictments do not necessarily remain bare; bare indictments can result in actual apprehensions. The Arrow Tech case study involves a seemingly "bare" indictment that led to the arrest of the cyberattacker Nima Golestaneh. Since Golestaneh subsequently pled guilty and was convicted, the seemingly "bare" indictment actually resulted in enforcement of the formal punishment for the crimes he pled guilty to committing. I argue

that the publicization of his arrest, guilty plea, and punishment deterred this convicted cyberattacker's accused co-conspirators from committing further cyberattacks because Golestaneh's co-conspirators realized that they too could be arrested, convicted, and formally punished. Thus, bare indictments' imposition of a contemplable risk of apprehension – which, in turn, also imposes a contemplable risk that the *formal* punishment for the crime will be enforced – serves as a 'backstop' of sorts. Raising the adversary's expected probability of cost – with the cost here being formal punishment, not just informal sanctions – means that bare indictments can deter cyberattacks not only via imposing informal sanctions, but also via imposing the risk of apprehension and of formal punishment. This aspect of bare indictments explains the achievement of a deterrent effect beyond the scope of the core theory.

Section 6.3. examines the Mabna Institute case study, another case involving an unexpected deterrent result that contradicts the theory's predictions. The accused cyberattackers in this case were arguably primarily motivated by prestige-seeking, which means that the theory predicts that they would be deterred by bare indictment. In actuality, a bare indictment failed to deter them. Furthermore, even though there was evidence that the accused cyberattackers had been contracted to carry out cyberattacks at the direction of the Iranian state, the issuance and publicization of the bare indictment did not deter at the nation-state level but rather provoked an enraged response from the Iranian state, wherein Iran essentially reaffirmed its commitment to proceeding with these types of cyberattacks. Indeed, empirical data indicates that the arguably prestige-seeking defendants in this case did not cease their cyberattacks, and instead have been cyberattacking at an even higher rate. I explain this contrary result by arguing that the U.S.

government's simultaneous issuance of economic sanctions against the indicted cyberattackers compromised the deterrent effect of the bare indictment. The discussion of the Mabna Institute case study should be of especial interest to policy practitioners, as the details of this case study cut against many scholars' competing contention that economic sanctions should always be deployed in conjunction with 18 U.S.C. § 1030 bare indictments. A CDT analysis suggests that imposing formal consequences in conjunction with an indictment may eliminate any further expected costs for adversaries to fear; as seen in the Mabna Institute case study, so doing undermines the deterrent effect of informal sanctions.

In this chapter demonstrating specialized facets of the theory on bare indictments' deterrent effect, both of the two case studies involve Iranian nationals. To identify prestige-seeking motives for cyberattacks in this Iranian context, Section 6.1. determines what the Iranian state considers to be markers of prestige.

6.1. Defense Capability as Prestige in Iran's Foreign Policy

My arguments as to whether a cyberattack allegedly perpetrated by an Iranian actor is or is not prestige-seeking rest on the following premise: Iran considers defense capability, particularly aerospace defense capability, to be a symbol of national prestige. Based on this premise, if a cyberattack can be technically attributed to an Iranian actor, then the cyberattack's targeting of data regarding defense materiel specifications can be interpreted as an indication of prestige-seeking.

What foreign policy actions by Iran support this premise? Overall, Iran's pursuance of defense capability for its prestige benefit beyond its practical benefit is evidenced by observing that Iran frequently signals its defense capability much more publicly than

would be expected if Iran saw defense capability predominantly in terms of practical firepower. To account for an asset's practical benefits and establish whether a state values an asset for its prestige benefit, Deborah Welch Larson and Alexei Shevchenko look to the extent to which a state publicizes its ownership of the asset (2019, 235). A state's effort and cost in publicizing its ownership of the asset is inconsistent with a contention that the state is "solely interested" in this asset for its "economic benefits" (2019, 235), as this effort and cost would serve no purpose. In accordance with a contention that Iran sees its defensive capability as a symbol of national prestige, Iran has continually conducted highly visible and highly publicized ballistic missile tests (Ajili and Rouhi 2019).

Iran's projection of national prestige via the use of its defense capability is also demonstrated by actions that could be colloquially described as 'overkill': demonstration of its defensive capability beyond that which is necessary to achieve a practical objective. For a state solely interested in practical benefit, these costly signals would be exorbitant. A recent example is Iran's response to the U.S.'s January 2020 killing of Qasem Soleimani, the leader of what the U.S. had deemed a terrorist group (Lim 2020, 157). As Kevjn Lim describes, "Iran responded with calibrated barrages of ballistic missiles on US forces deployed at two Iraqi air bases, causing traumatic brain injury to more than 100 US military personnel" (Lim 2020, 157). Surprisingly, even though many of these missiles accurately hit buildings within the bases, Iran's missile strikes did not result in any reported casualties and did not result in widespread infrastructural damage to the bases (Chappell 2020; Brumfiel and Welna 2020).

Why did Iran mount these missile strikes upon the U.S. bases yet seemingly squander the missile strikes' obvious capacity to cause fatalities and destruction? Of three

possible explanations one might consider, prestige is the most consistent with the facts at hand. The first explanation, that Iran did not have the technological capability to accomplish the objective of taking the U.S.'s bases out of play, is unlikely given the capability demonstrated by Iran's successive ballistic missile tests. Relatedly, a second explanation – that Iran did intend to cause fatalities and destruction, but its missiles malfunctioned – is also unlikely given the capability demonstrated by Iran's tests. Moreover, it seems implausible that, among Iran's series of missile strikes in January 2020, not one of Iran's missiles functioned properly; this suggests that Iran was not, in fact, attempting to cause fatalities and destruction. A third possibility is that Iran mounted the ballistic missile strikes not only as a communicative statement of its outrage at the U.S.'s action, as making a communicative statement could be accomplished through less costly means; but also as a signal of its comparative superiority vis-à-vis the U.S. In other words, Iran was signaling its status. This is the explanation favored by analysts quoted in an *NPR* report from January 8, 2020 (Brumfiel and Welna 2020). Larson's and Shevchenko's method may be extended to evaluate alternative explanations that do *not* include prestige. If the Iranian state's use of its defensive capability were *not* seeking to establish its prestige, then Iran's depletion of its highly accurate missiles would be a waste of resources that accomplished no practical objective, as the missile strikes caused far less damage than was well within Iran's missile capability. With respect to the January 2020 ballistic missile strikes, it is unlikely that Iran used its defensive capability to achieve the objective of causing fatalities and destruction; rather, Iran's defensive capability was mainly used to send a message regarding Iran's superiority, demonstrating that Iran *could* have caused fatalities and destruction.

Interestingly, Iran's foreign policy goal of using its defense capability to signal prestige is part of a sweeping MDT strategy that not only regards defense capability as a means of domestic economic growth, but also instrumentally uses the projection of prestige to deter international military attacks. Marcus Solarz Hendricks' characterization of the Iranian state's overarching objective as "regime survival" shows that both the practical defensive benefit and symbolic prestige benefit of defensive capability are reflective of Iran's prestige-seeking behavior and its sensitivity to humiliation: "Susceptible to internal pressures and external humiliation, the survival of the Islamic Republic now demands… the ability to defend itself from potentially crippling attacks by regional and global rivals" (2021). Likewise, Jose Miguel Alonso-Trabanco writing for the *Geopolitical Monitor* positions Iran's development of its defense technology sector, especially aerospace defense, as having both domestic benefits of economic growth and international benefits of prestige projection (2022). Hadi Ajili and Mahsa Rouhi tie these facets of Iranian foreign policy together in an argument that Iran's prestige-seeking behavior in continually publicizing its defensive capability reveals that Iran's overarching objective is to deter military attacks (2019). The Iranian state sees prestige, then, as a crucial part of Iran's MDT strategy. Iteratively demonstrating not just Iran's defensive capability, but more precisely its defensive capability's relative "superiority" over other nations' – especially the U.S.'s – is integral to Iran's policy objective of achieving military deterrence (Ajili and Rouhi 2019).

This brief overview of Iranian foreign policy provides evidence for the premise that the Iranian state sees defensive capability as a symbol of national prestige. Using Larson's and Shevchenko's qualitative method, the contention that a nation-state values an asset for

their prestige benefit can be directly tested for by reference to publicizing the ownership of this asset to an extent beyond that which would achieve a practical benefit other than prestige. Furthermore, if the Iranian state did *not* see demonstrations of its defensive capability as projections of prestige, then a major component of Iran's deterrence-focused military strategy would be rendered inexplicable. Iran's need to demonstrate superiority for domestic regime preservation and in achieving military deterrence rests on the prestige value of its defensive capability.

6.2.0. Bare Indictments Deter Because They Do Not Necessarily Remain "Bare" [IRAN-01] [IRAN-03]

On July 17, 2017, the DOJ OPA announced the unsealing of an indictment against two Iranian nationals, Mohammed Saeed Ajily and Mohammed Reza Rezakhah. The indictment, which had been filed on April 21, 2016, alleged that the two individuals had violated 18 U.S.C. § 1030(a)(2) by obtaining unauthorized access to the computer systems of Arrow Tech, a U.S. company that manufactured software for defensive weapons (*Ajily* indictment). This case study serves as an example of how bare indictments can deter by raising the potential offenders' expected probability of cost if they are to attempt further cyberattacks. To understand the process by which bare indictments can increase expected probability of cost, it is necessary to start the narrative before the indictment's April 2016 filing. As was made evident by the November 2013 arrest of Rezakhah's and Ajily's alleged co-conspirator Nima Golestaneh and the December 2015 announcement of Golestaneh's plea bargain agreeing to turn against his co-conspirators in the Arrow Tech cyberattacks, one reason bare indictments deter is that they do not necessarily remain 'bare.'

This section proceeds as follows. As with other case studies, I first analyze the information contained in the indictment and the surrounding circumstances regarding the cyberattack to determine the perpetrators' motive. Although I find that the evidence on motive renders an unclear result, I show that the bare indictment's function in increasing the expected probability of cost can apply irrespective of the profit-seeking, thrill-seeking, or prestige-seeking motive. To explicate this process, I review the circumstances of Golestaneh's arrest in 2013 and extradition in 2015 notwithstanding his Iranian nationality. I analyze why Ajily's and Rezakhah's fear of being arrested – as was their alleged co-conspirator – deterred them from perpetrating any further cyberattacks. This case study hence elucidates and supports CDT's contentions on the probability of apprehension itself as a deterrent. I conclude this section by reflecting on a crucial policy implication regarding a general feature of bare indictments that enables them to deter cyberattacks. Bare indictments are "bare" because it appears highly unlikely that an indictment of a foreign national from a nation that has no extradition treaty with the U.S. will ever lead to an arrest, much less the imposition of any formal punishment as a result of the indictment. Despite this low likelihood, this case study demonstrates that bare indictments have led to arrests in actuality; thus, the prospect that they too may be arrested deters potential cyberattackers.

6.2.1. Mixed, Indeterminate Motives of Arrow Tech Cyberattackers

The details of the indictment, when contextualized against Iran's foreign policy goals, show that the alleged perpetrators of the cyberattack against Arrow Tech likely had mixed profit-seeking, prestige-seeking, and perhaps also thrill-seeking motives. Part of the

reason for this mixed motivation is that the two indicted individuals fall into a liminal category when assessing whether they are best categorized as state-sponsored or non-state actors. The indictment alleges that Ajily directed Rezakhah to handle the technical aspects of breaking through Arrow Tech's encryption; Ajily would handle the distribution of the software, "in contravention of Western sanctions against Iran," to be sold on "the Iranian market, including for Iranian military and government entities" (*Ajily* indictment, line item 5). The indictment continues, "In addition to payment, [Ajily] received certificates of appreciation for his work from several of the Iranian government and military entities" (*Ajily* indictment, line item 5). The indictment does not allege that Ajily acted at the direction of the Iranian state. Based on this information, these cyberattacks would best be categorized as "state-encouraged" on Jason Healey's seminal "Spectrum of National Responsibility for Cyberattacks" (2011). On Healey's spectrum, state-encouraged cyberattacks fall midway as to state responsibility, and Healey defines state-encouraged as "third parties control and conduct the attack, but the national government encourages them to continue as a matter of policy" (2011, 60). What the indictment describes as "certificates of appreciation" from Iranian state agencies meets this definition of nation-state encouragement.

The information about paper commendations from the Iranian state suggests that Ajily and Rezakhah might have been primarily motivated by thrill-seeking, or the prospect of gaining positive emotions as a consequence of successfully executing the cyberattack; conversely, the other details suggest that prestige-seeking and profit-seeking may have been the indicted individuals' motives. The target of the cyberattack was an aerospace defense company. Although the indictment does not lay out a full analysis (*Ajily*

indictment, 7, Count 2) of why the cyberattacks arguably satisfy the elements necessary to allege a violation of 18 U.S.C. § 1030(a)(2), the target's activities in developing aerospace defense software is likely why 18 U.S.C. § 1030(a)(2) – specifically 18 U.S.C. § 1030(a)(2)(C), on obtaining information from a "protected computer" – applies. According to 18 U.S.C. § 1030(e)(2)(A), "protected computer" can mean "a computer… used by or for… the United States Government and the conduct constituting the offense affects that use by or for… the Government." The Arrow Tech software's designation as a "defense article," as stated in the indictment (*Ajily* indictment, 1), meant that the unauthorized access to Arrow Tech's computer systems and obtaining information about its software qualified as pertaining to the U.S. government's use of Arrow Tech's computer systems.[19] As examined in subsection 4.3.0's discussion, developing aerospace defense capabilities is a main prestige-seeking foreign policy goal for the Iranian state. Moreover, based on the indictment's allegation that Ajily specifically "advertised what he referred to as his group of software hackers… and their ability to circumvent Western sanctions against Iran by hacking the servers of software manufacturers and cracking software protections in order to obtain software for Iranian entities" (*Ajily* indictment, line item 17), Ajily may have been attempting to demonstrate his group's superiority over the West. Considering that Ajily allegedly touted his team as being able to circumvent Western sanctions and that his team allegedly sought to obtain weapons software for Iranian state entities, prestige-seeking may have been the primary motive for the cyberattacks.

[19] Alternatively, Arrow Tech's computer systems could have qualified as protected computers under 18 U.S.C. § 1030(e)(2)(B), "a computer… used in or affecting interstate or foreign commerce or communication," as Arrow Tech's "business in interstate or foreign commerce" was established on the first page of the indictment (*Ajily* indictment, 1).

Another argument is that some circumstances indicate that the cyberattacks were primarily motivated by profit-seeking. The indictment does not allege that the misappropriated software that Ajily and Rezakhah obtained from their unauthorized access to Arrow Tech's computers was then donated or otherwise tendered to the Iranian state agencies free of charge. Rather, the indictment alleges that Arrow Tech's proprietary software was put up for sale on the Iranian market to the highest bidders (*Ajily* indictment, 4). Moreover, even though defense capabilities can be symbols of prestige, they also have a functional component. Based on this information, it is possible that the desire for monetary profit might have predominated over national pride or emotional thrill. These details indicate that the perpetrators may have been primarily profit-seeking.

6.2.2. Actual Apprehension as Deterrence

Notwithstanding that the exercise of separating out indicators of motive can serve as a useful template, motive was not a determinative factor in the success of the deterrent effect in this case. This is because the deterrent effect of the bare indictment was mainly achieved not by directly frustrating the motives of the alleged cyberattackers, but rather, by outweighing any expected weighted benefits that the perpetrators would have expected to receive from committing further cyberattacks. While bare indictments often deter by directly countervailing the status-seeking motive and hence decreasing a cyberattacker's expected benefit, in this case the bare indictment deterred by increasing the adversary's expected probability of cost. An analysis of the events leading up to the indictment supports an argument that the arrest and guilty plea of alleged co-conspirator Golestaneh

served as an example that persuaded Ajily and Rezakhah that the expected risk of being arrested would outweigh the expected benefit from perpetrating further cyberattacks.

Although it may arguably be unlikely that a foreign individual will be arrested as a result of a bare indictment, the issuance of a bare indictment always carries a potential for arrest. This resonates with a unique feature to which Garrett Hinck and Tim Maurer call attention. According to Hinck and Maurer, the third of three ways that "criminal charges differ from many other ways of responding to cyber incidents" is that criminal charges "are intended to enable arrests as opposed to just being public statements" (2020, 529). Relatively little study has been devoted to the "bare" indictments that do result in arrests of alleged foreign cyberattackers (Hinck and Maurer 2020, 527), yet – as this case study illustrates – this feature is an integral component of criminal charges' deterrent force.

On December 2, 2015, three events occurred that changed the trajectory of the Arrow Tech hacking case. First, Golestaneh and his legal counsel signed a guilty plea to the crime of "Fraud in Connection with Computers" in violation of 18 U.S.C. § 1030(a)(2).[20] The agreement specified that Golestaneh "agrees to plead guilty because he is, in fact, guilty of the above crimes" (*Golestaneh* plea agreement). Under the conditions of the plea agreement, Golestaneh was obligated to "refrain from committing any further crimes, whether federal, state or local" (*Golestaneh* plea agreement). Since the wording of this condition covered all applicable U.S. crimes, this condition imposed on him the legal obligation not to commit any further cyberattacks in violation of 18 U.S.C. § 1030; if he violated this condition, then the condition on the U.S. government's agreement not to further prosecute him would not be valid and the U.S. could proceed with trial.

[20] In the same plea agreement, Golestaneh also pled guilty to wire fraud in violation of 18 U.S.C. § 1343.

Second, as indicated by the stamp of the clerk of court, Golestaneh's plea agreement was filed with a U.S. federal district court, specifically the U.S. District Court for the District of Vermont (*Golestaneh* plea agreement). Having been placed on record, the plea agreement could serve as the basis for the third event, which is perhaps the most decisive of the three in achieving the deterrent effect. This third event was the DOJ OPA's public announcement that Golestaneh had submitted a guilty plea. The press release, which was likewise dated December 02, 2015 and marked "FOR IMMEDIATE RELEASE," described Golestaneh as an "Iranian national" and contained two seemingly unassuming sentences that, I argue, carry significant deterrent force: "In November 2013, Golestaneh was arrested in Turkey in connection with the indictment. He was extradited to the United States on Feb. 12, 2015 pursuant to a Mutual Legal Assistance Treaty" (DOJ OPA, December 02, 2015).

Four crucial inferences and observations can be made from this brief passage. One, the passage implies that Golestaneh had been subject to his own bare indictment. Oddly, even though the sentence reads "in connection with the indictment," nowhere else in the text of the press release is reference made to Golestaneh's having been indicted; therefore, it is an implicit rather than explicit detail. When the implicit detail about "indictment" is read in conjunction with Golestaneh's status as a foreign national from a country with no bilateral extradition treaty with the U.S., the inference can be made that the indictment was – at the time of issuance – characterizable as a 'bare' indictment. Two, resonating with Hinck's and Maurer's third unique function of criminal charges, the passage indicates that an indictment enabled Golestaneh's arrest. Three, the passage makes clear how, despite it having been highly unlikely that the bare indictment issued against Golestaneh would ever

lead to his arrest, he was nevertheless arrested. Golestaneh was arrested because, at the time of his arrest, he was physically located in a country that *did* have a bilateral extradition treaty with the U.S.[21] Four, after his arrest in late 2013, Golestaneh was apparently detained or otherwise in a state of legal 'limbo' for more than a year before Turkey extradited him to the U.S.

CDT predicts that the inferences and observations that could be straightforwardly made from the public announcement of Golestaneh's arrest would serve as a deterrent measure against other cyberattacks. Beccaria and Bentham explain that a punishment cannot be kept secret, as it then has no deterrent effect; conversely, the more a punishment is made publicly known, the more effectively it is expected to deter. According to classical CDT, publicizing a punishment known is intended to convince others that the same fate would likely befall them if they were to commit like offenses.

[21] Another inference, regarding a finer point of international criminal procedure, may be of interest to some readers: Turkey likely 'voluntarily' cooperated with the U.S. on arresting Golestaneh. The press release makes reference to "a Mutual Legal Assistance Treaty." "Mutual Legal Assistance Treaty" ("MLAT") is a general descriptor. According to U.S. Congressional records, the extradition treaty with Turkey is entitled the "TREATY WITH TURKEY ON EXTRADITION AND MUTUAL ASSISTANCE IN CRIMINAL MATTERS." Thus, the bilateral extradition treaty and the MLAT are one and the same in the case of the U.S.'s treaties with Turkey. This is not necessarily true with respect to all countries. MLATs, on their own, do not usually *obligate* the signing nations to cooperate; their function is to provide a "framework" that *facilitates* information sharing and cooperation between the law enforcement officers of the respective nations (MacCormack 2009, 464, at footnote 96). A strict reading of the quoted passage indicates that MLAT provisions facilitated Golestaneh's arrest. If this is true, then it can be inferred that it is likely Turkey not only complied with its legal obligation to extradite Golestaneh, but also cooperated with the U.S. in locating Golestaneh so that he could be arrested – notwithstanding that Turkey was not legally obligated to do so. The significance of this inference, for deterrent purposes, is that it demonstrates that foreign nations may cooperate with U.S. law enforcement even though they are not legally obligated to do so. Hence, the deterrent effect of bare indictments may be enhanced for potential offenders who are cognizant of this inference; there is a chance that foreign nations can choose to cooperate with the U.S. in making arrests. However, this inference is based on specialized knowledge of international treaty law and international criminal procedure; the inference may not have any additional deterrent effect to most potential offenders, who may find this inference overly esoteric when made from the Golestaneh case. A clearer example can be found in the case of Roman Seleznev, who was arrested in the Maldives – once thought to be a safe haven for Russian oligarchs. I discussed Seleznev's case in Chapter 5.

Under Beccaria's and Bentham's theories, the press release about Golestaneh's arrest is an optimal deterrent measure. The press release established the negative consequence that befell Golestaneh as a result of his having committed cyberattacks. This negative consequence was his arrest, which would previously have been thought so unlikely as to be an impossibility. The arrest led to Golestaneh's guilty plea, which meant that his case would proceed directly to the sentencing phase. Golestaneh's plea agreement outlines what the sentencing phase entails; in the sentencing phase, the court could order Golestaneh's imprisonment, order that a monetary fine be levied against him, and order that he be required to pay restitution, i.e. compensation, to the victims of his crime (*Golestaneh* plea agreement). Furthermore, the arrest triggered negative consequences corresponding to the informal sanctions that are imposed upon apprehension; the arrest meant that Golestaneh was then subject to the applicable criminal procedure, which included his being detained in Turkey for over a year before being extradited.

Especially to Golestaneh's co-conspirators – the then-unknown individuals who had, in fact, committed the very same offenses as had Golestaneh – Golestaneh's arrest would serve as an example of what could happen to them if they too were arrested. The press release established that arrest itself was a negative consequence, as Golestaneh was detained in Turkey for over a year. The press release adjusted the seemingly infinitesimal probability of being arrested to a contemplable risk, since Golestaneh was arrested and extradited despite his being a foreign national of a state that was not legally obligated to extradite to the U.S. Significantly, the press release established that the negative consequences that were imposed on Golestaneh all stemmed from his bare indictment. In sum, the press release affirmed the expected cost of committing further cyberattacks like

the ones Golestaneh had committed and – most significantly – raised the expected probability of such cost to a contemplable risk. The press release would hence be expected to convince any individual subject to a bare indictment under similar circumstances that the individual would probably suffer negative consequences like those that befell Golestaneh – unless the individual could avoid being arrested.

Avoiding arrest – or apprehension – meant that an indicted individual would have to refrain from executing further actions that subjected them to high risk of detection. A close examination of the process in this case study serves as an illustrative example to support Nagin's contention that the probability of apprehension, rather than the probability of conviction or sentencing, is determinative in a potential offender's risk calculus (2013). This is partially because, as suggested by West's study (2003), apprehension itself triggers the cost of practical consequences such as detainment. Practical consequences apply even when assuming that a given individual subjectively would feel no negative emotional consequences of shame from being arrested, would be indifferent to any loss of prestige, and would not care about being socially ostracized.

Having discussed why the press release regarding Golestaneh's arrest was an optimal deterrent measure and how it would be expected to deter other offenders by instilling in them the fear of apprehension, it can now be observed that the facts of the case study are consistent with predictions. The indictment against Ajily and Rezakhah expressly referred to Golestaneh as a "co-conspirator" (*Ajily* indictment). As soon as the bare indictment was issued, it could serve as the basis for Ajily's and Rezakhah's arrests. The possibility of arrest would become an especially significant expected risk for Ajily and Rezakhah after the bare indictment was unsealed, as the public announcement of the

indictment made it known that Ajily and Rezakhah had been named as alleged co-conspirators. It was therefore made clear to Ajily and Rezakhah that if they were arrested, they would be subject to similar practical negative consequences as was Golestaneh. With every element of an optimal deterrent measure having been present, CDT would predict that Ajily and Rezakhah would be deterred from perpetrating any further cyberattacks, because committing more cyberattacks could reveal their location via technical attribution. Being deterred from perpetrating further cyberattacks is one component of avoidance of arrest, as the deterrent effect here would be achieved via convincing the named individuals that costly consequences were likely to result from their apprehension. Overall, then, the prediction is that nothing more would ever be heard from Ajily and Rezakhah. In avoiding arrest, they would not only refrain from further cyberattacks, but also go completely silent – 'keep a low profile,' so to speak.

While the absence of evidence on recidivist cyberattacks from Ajily or Rezakhah may not be entirely dispositive of a competing contention that the bare indictment failed to deter Ajily and Rezakhah, the absence of evidence fits with the prediction that the bare indictment did indeed deter Ajily and Rezakhah by instilling in them the fear of arrest. Open-source research yields no relevant results regarding information on the two individuals' activities or confirmed whereabouts since the unsealing of their indictment. If the fear of arrest were not at play in deterring these individuals, this would be a surprising result. Although the counterargument could be made that the individuals may have refined and improved their skills such that they can commit further cyberattacks without being detected, this interpretation does not comport as well with the absence of information, since this absence is itself atypical. In a context where reports and findings regarding

technical attribution are usually published, absence of evidence on a known cyberattacker's suspected activities would be unusual unless the cyberattacker is, in actuality, no longer active. Despite that technical attribution may not be timely, technical attribution of a cyberattack can almost always be made, and private firms tend to make their findings public. Thus, if Ajily and Rezakhah were perpetrating any further cyberattacks, the cyberattacks would have to be small in scale so as to not receive resources devoted to their technical attribution. Ajily and Rezakhah have apparently been deterred from committing large-scale cyberattacks that would be likely to call attention to their location, as so doing would risk their arrest.

This case study, then, highlights one path by which bare indictments deter: they raise the indicted individual's expected probability of arrest, with arrest itself carrying practical negative consequences. Publicizing Golestaneh's arrest made it clear to his co-conspirators and warned other potential offenders that, even if the indictment were a "bare" indictment issued against a foreign national from a state without a bilateral extradition treaty with the U.S., an arrest could still be made. As with other measures of criminal deterrence, it cannot be guaranteed that potential offenders will necessarily be deterred – but the press release, as an optimal deterrent measure that integrated CDT's most important components, maximized the chances of achieving a deterrent effect. In accordance with predictions, it seems that the deterrent measure of bare indictments against alleged co-conspirators did deter them from recidivist perpetration of cyberattacks.

This case study is a deterrence success. From a policy standpoint, a recommendation is to follow the case study by publicizing any future arrests of individuals who have been subject to bare indictment. Doing so moves the ball forward on deterrence,

since it tends to increase potential offenders' expected probability of cost. Moreover, by affirming that apprehension itself is costly, cyberattackers will be deterred from recidivist offenses, given that they expect that committing further cyberattacks is likely to reveal their location and hence lead to their arrest.

This proposition can be generalized to classical CDT's contention that potential offenders are deterred from committing offenses when they expect that committing offenses will likely make them incur a cost that, in their estimation, will outweigh the benefit of the offense; however, the case study lends the contention further particularity. A bare indictment can deter alleged cyberattackers from perpetrating further cyberattacks because a bare indictment can make the alleged cyberattackers expect that so doing will likely make them incur the informal sanctions triggered by apprehension.

What happens, then, if an alleged cyberattacker – against whom a bare indictment has already been issued – has no reason to expect that perpetrating further cyberattacks will make them incur additional cost, and instead expects that no additional cost can be incurred? The premature imposition of cost is, I argue, the reason for the deterrence failure in the next case study.

6.3.0. Nothing More to Fear: Why Premature Deployment of Economic Sanctions Undermines the Deterrent Effect of Bare Indictments [IRAN-05]

On March 23, 2018, the DOJ OPA and the USAO SDNY each publicly announced the unsealing of an indictment charging nine Iranian individuals with violations of 18 U.S.C. § 1030. These press releases also stated that, on the very same day, the U.S. Treasury's Office of Foreign Assets Control ("OFAC") imposed economic sanctions on each of the nine

individuals and the Mabna Institute, the Iranian company under whose purview the individuals were alleged to be conducting cyberattacks (USAO SDNY, March 23, 2018; DOJ OPA, March 23, 2018). Although the indictment provoked an indignant response from the Iranian state, Iran was apparently undeterred, as Iran's indignant response doubled down on Iran's commitment to commit similar cyberattacks. Years later, a 2021 report from a private security firm would provide evidence that Iran's commitment was not just cheap talk; the report shows that throughout 2020, the Mabna Institute not only continued to commit cyberattacks like those on which the U.S. based its indictment and economic sanctions, but also has expanded the frequency and scope of its operations. Why was the Mabna Institute undeterred despite being a prestige-seeking actor who was subject to a bare indictment?

I argue that the U.S.'s strategic misstep in prematurely deploying economic sanctions against the Mabna Institute and its affiliated individual actors did not reinforce, but rather did undermine, the deterrent effect of bare indictments. Contrary to scholars who urge that bare indictments should always be followed closely by sanctions in order to achieve the deterrent principle of "consistency" and maximize the deterrent effect against alleged cyberattackers, I draw from the principles of classical CDT and from contemporary studies on the deterrent effect of economic sanctions to show that imposing rather than threatening sanctions counterproductively eliminated the expected cost that the Mabna Institute could otherwise have factored into its cost-benefit calculus for committing further cyberattacks. I also examine the nature of the Mabna Institute's cyber operations to show why economic sections not only fail to deter, but also fail to disrupt its hostile cyber operations. In crafting a policy that effectively deters cyberattackers, the Mabna Institute

case study serves as a cautionary example. Instead of always following bare cyber indictments by cyber economic sanctions in presumed service of 'consistency' or 'norm-setting,' a policy question that should be assessed going forward is what additional disruptive and deterrent effects economic sanctions are likely to have on the specific actor against which they are imposed, since an inefficient failure to achieve specific deterrence may subvert any general norm-setting deterrent effect that may otherwise have resulted.

This section proceeds as follows. First, I establish the prestige-seeking motive of the nine indicted individuals who were affiliated with the Mabna Institute. Second, I review the prevalent argument that bare indictment of cyberattackers should always be followed by economic sanctions. Third, I refer to CDT principles to support the contention that the *threat* of economic sanctions has a greater deterrent effect than the actual imposition of economic sanctions. Adding economic sanctions to bare indictment could hence be seen as duplicative of some aspects of deterrence and undermining of other factors in the cost-benefit calculus. Fourth, I study the Mabna Institute's operations to show that, as could have been predicted in 2018 based on the information that was known at the time, economic sanctions would be unlikely to disrupt this specific actor. I use this case study to argue against a blanket approach to economic cyber sanctions; I instead suggest that more attention be devoted to conducting an individual analysis of what additional effect economic sanctions may have to augment bare indictments.

6.3.1. A Failure to Deter Prestige-Seeking Cyberattackers

The academic nature of the cyberattacks' victims, of the alleged data theft that the cyberattacks were instrumental to executing, and of the Iranian universities that allegedly

profited from such data theft supports an argument that the actors who mounted these cyberattacks were primarily motivated by prestige-seeking. As stated in the DOJ OPA's press release, this indictment concerns a "coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund" (DOJ OPA, March 23, 2018). The indictment alleges that the Mabna Institute, acting through its indicted affiliates, conducted this "coordinated campaign" "at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps" (*Rafatnejad* indictment, 2); thus, the Mabna Institute can clearly be characterized as an agent of the Iranian state. The indictment continues by alleging that "the members of the conspiracy compromised thousands of accounts belonging to professors at victim universities and targeted academic data and intellectual property for theft" (*Rafatnejad* indictment, line item 2). As discussed in Chapter 2, data has monetary value, but the academic quality of the data that was taken coincides with the Iranian state's view of scientific advancement as gaining national prestige. The DOJ OPA's press release highlights that the data was taken primarily for the benefit of Iranian academic institutions: "Gholamreza Rafatnejad and Ehsan Mohammadi, [two of the nine] defendants, founded the Mabna Institute in approximately 2013 to assist Iranian universities and scientific and research organizations in stealing access to non-Iranian scientific resources" (DOJ OPA, March 23, 2018). Although the indictment implies that the Mabna Institute had a contractor-like relationship with the IRGC and that the Mabna Institute was being hired for pay rather than providing its services free of charge

(*Rafatnejad* indictment), it is significant that the taken intellectual property was not usually monetized by being placed on sale to the highest bidders, but rather, was then tendered to the Iranian academic institutions. These descriptive details suggest that the actors who committed these cyberattacks were primarily motivated by prestige-seeking.

Under this project's theory of bare indictments, the bare indictment would have been predicted to achieve a deterrent effect against the Mabna Institute. By labeling the Mabna Institute's affiliates as criminal outcasts, the bare indictment should have convinced the Mabna Institute that any further cyberattacks would fail to achieve the objective of prestige. The prediction is that the bare indictment would achieve specific deterrence by lowering the Mabna Institute's expected benefit of prestige. Moreover, since the indictment established that the Mabna Institute was acting upon direct orders from the IRGC and therefore the Iranian state, attribution theory would have predicted that the deterrent effect would extend upward to the Iranian state as well.

As predicted, the Iranian state reacted indignantly – but contrary to predictions, its indignant response pronounced that it was undeterred. According to a news report from Tehran, Iran on March 24, 2018, "Foreign ministry spokesman Bahram Ghassemi called the accusations 'false.' 'Iran condemns the United States' provocative, illegal and unjustified actions, which are a major new sign of the hostility and animosity of US leaders towards the Iranian people,' he said in a statement on the ministry's website. 'They will not prevent the scientific development of the Iranian people'" (AFP 2018). By promising that Iran would continue the "scientific development" that the alleged cyberattacks had been instrumental in achieving, Ghassemi's statement implied that Iran would continue its prestige-seeking

behavior in mounting cyberattacks to obtain intellectual property from the U.S.'s and other nations' academic institutions.

A 2021 report by the Insikt Group, a research organization working within the private cybersecurity intelligence firm Recorded Future, proved Ghassemi's pronouncement and provides clear evidence that the Mabna Institute was undeterred. In this report, which was made publicly available, the Insikt Group stated that throughout the 2020 calendar year the Mabna Institute had increased the rate of its cyberattack attempts (Insikt Group 2021, 1-2). The cyberattacking activities outlined in the report were the same as those for which the Mabna Institute's affiliates had been indicted in 2018; the Mabna Institute's targets were research professors and academic institutions in the U.S. and other nations, the Mabna Institute was attempting to take academic intellectual property (Insikt Group 2021, 2), and – as will be further discussed below – the Mabna Institute used the same "phishing tradecraft" (Insikt Group 2021, 3).

6.3.2. Raising and Rebutting Arguments on Simultaneous Imposition of Economic Sanctions

This result – that the Mabna Institute was clearly undeterred and undisrupted – may cast doubt on arguments that economic sanctions should be imposed in tandem with bare indictments against alleged cyberattackers. Trevor Logan espouses this view in a 2019 policy brief entitled "U.S. Should Indict and Sanction Cyber Adversaries." Speaking favorably of the "use of sanctions to complement indictments," Logan argues, "pairing indictments with sanctions could be a more effective means of holding adversaries accountable. Sanctions would put more pressure on the governments sponsoring cyberattacks by restricting the funds and access to technology that facilitate them" (Logan

2019). Logan's argument is adopted by Ellen Pruitt (2021), writing in the *University of Baltimore Law Review*. In arguing that bare indictments do not deter cyberattacks, Pruitt concludes, "The best apparent solution is for the congruent use of both sanctions and indictments… it is unclear why it is not done consistently in response to cyberattacks on U.S. assets" (Pruitt 2021). A milder version of the argument – that a significant component of bare indictments' utility is that they "pave the way" for economic sanctions – is made by David Hechler, writing for *Lawfare* (2021).

Interestingly, the arguments for "sanctioning all indicted cyber operatives" have directly invoked the deterrence rationale (Logan and Patel 2020b). In Logan's and Patel's 2020 data analysis of the FDD CCTI dataset, Logan and Patel further argue, "by constraining access to financial resources and changing the aggressor's cost/benefit dynamics, sanctions likely would help establish a stronger deterrence posture" (Logan and Patel 2020b). Logan also argues that always imposing economic sanctions in conjunction with issuing bare indictments accomplishes general deterrence via the mechanism of norm-setting: "An enforcement regime applied consistently to all foreign actors would signal to adversaries what the United States considers acceptable behavior in cyberspace" (2020b). Logan and Patel cite, as do analysts Allison Peters and Pierce MacConaghy in a 2021 memorandum entitled "Unpacking U.S. Cyber Sanctions," a quote from a March 2020 report of the U.S. Congress' Cyberspace Solarium Commission that highlights the importance of 'consistency.' While my reading of the report does not find that the Commission necessarily advocates for the imposition of economic sanctions against cyber actors whenever feasible, the Commission does present economic sanctions as one of the "tools of state power" that may be leveraged for achieving general deterrence (2020, 46); the Commission expressly points

to economic sanctions as a means of norm-setting (2020, 3). Although Peters and MacConaghy acknowledge that general theoretical arguments on cyber sanctions may be promising, they call for critical assessments of the impact of the cyber sanctions that have already been levied, as too little evidence supporting or disproving actual effectiveness exists to make a policy recommendation beyond devoting more resources to assess "whether these cyber sanctions have had an impact in changing their target(s) behavior or achieving other established goals" (2021).

The failure of cyber sanctions to alter the Mabna Institute's cyberattacks shows that the application of cyber sanctions cannot be one-size-fits-all. If – as I argue – a deterrent effect would likely already have been achieved by a bare indictment, the principles of CDT would militate against the imposition of economic sanctions; CDT predicts that the additional quantum of punishment would be extraneous and hence suboptimal.[22] Classical CDT also predicts that if a punishment is imposed before the threat of such punishment was communicated to the actor, this punishment cannot have a deterrent effect (Bentham 1830, 23-24).

6.3.3. The Threat, Not Imposition, of Economic Sanctions Deters

This resonates with some scholars' contentions that it is the threat, rather than the imposition, of economic sanctions that may achieve a deterrent effect; by contrast, it is exceedingly rare for imposed economic sanctions to achieve a deterrent effect. Threatening sanctions against an actor gives that actor an opportunity to change its behavior in attempting to avoid sanctions, whereas the actor has less incentive to change

[22] "A punishment is needless, where the purpose of putting an end to the practice may be attained as effectually at a cheaper rate" (Bentham 1830, 25).

its behavior once economic sanctions are already in place. Political scientists Dean Lacy and Emerson M.S. Niou illustrate this point by constructing a game-theoretic model of economic sanctions that distinguishes the "threat stage" from the "sanction stage" (2004, 35). Lacy and Niou show that "sanctions that are likely to succeed will do so at the mere threat of sanctions" (2004, 25). Thus, the imposition of economic sanctions only occurs when neither threat nor imposition would likely change the actor's behavior, since the purpose of imposition is then to establish the imposer's credibility; so that other actors do not see the imposer's future threats of economic sanctions as empty threats, actual imposition is necessary to signal that the threat of economic sanctions was not a bluff (2004, 38). Similarly, economist Daniel W. Drezner draws from the field of strategic interaction to show that "most successful uses of economic coercion should end before sanctions are imposed" (2003, 648). A threat of economic sanctions can often be determinative in the success of persuading an actor to change behavior; if the actor has already acquiesced, no additional deterrent effect is achieved by imposing the economic sanctions.

Actual imposition of economic sanctions can be unnecessary and therefore inefficient because the threat of economic sanctions would have sufficed. Even if the imposition of economic sanctions may be extraneous when a bare indictment has already been issued, why not impose them anyway if the resources are allocated to enforce them and the political will exists? I suggest that the Mabna Institute case study shows why imposition of economic sanctions may not only be extraneous, but also counterproductive. Scholars have invoked the expected cost-benefit calculus as a reason for justifying sanctions, but a reconceptualization shows why economic sanctions may undermine the

deterrent effect of bare indictments. As Hechler points out, bare indictments can "pave the way" for economic sanctions (2021); the bare indictment can hence be seen as communicating the conditional threat that economic sanctions will likely be imposed if the actor does not refrain from cyberattacks. If the imposition comes concurrent with the threat, the actor has no opportunity to contemplate the threat, much less comply in response. The deterrent effect that the bare indictment may have had is denied a chance to deter the actor.

Even beyond classical CDT's concern of inefficiency, conceptualizing economic sanctions in the cost-benefit calculus shows that the imposition of sanctions removes the cost an actor may otherwise have contemplated from committing further cyberattacks. A criminal punishment, such as a monetary fine or jail time, has a finite scope upon which further punishment can be added. For instance, if a fine of five hundred dollars is imposed on an actor who has been convicted of petty theft, the fine has a finite scope of five hundred dollars, and an additional fine may be imposed on the actor if the actor commits another petty theft and is convicted. If the actor is sentenced to a month of imprisonment, the jail sentence has a finite scope of a month, and more jail time may be added if the actor commits additional offenses and is convicted. By contrast, economic sanctions ordinarily do not have a finite scope; they do not 'end' after a specified time period. Also, there is no 'adding upon' economic sanctions of the type that were imposed on the Mabna Institute. Once a person – whether individual or entity – is added to OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), "their assets are blocked and U.S. persons are generally prohibited from dealing with them" (U.S. Department of the Treasury, "SDN Lists," 2022). If the person commits further offenses that could incur sanctions, their

recidivism may be noted, but the person has already been blocked; applying further economic sanctions to this person would have no practical effect. This type of economic sanction is binary; either the person is blocked, or not. When a person is completely blocked as a result of being added to the SDN List, there is no being 'additionally blocked' via the SDN List. Thus, a person that has been added to the SDN List can expect that if the person chooses to continue committing the offenses that incurred the imposition of economic sanctions, no further negative consequences will be imposed.

Not only do economic sanctions have no finite scope, but imposed economic sanctions are also difficult to lift (Haass 1998); therefore, the actor can expect no additional incentive to change its behavior. Before economic sanctions were imposed, the actor may have been willing to change its behavior in order to avoid economic sanctions. After economic sanctions are imposed, the actor no longer contemplates avoidance of sanctions; it seems a truism, but it should be noted that there is nothing further to deter the actor. The actor will be less inclined to change its behavior, because at that stage it is less likely that a change in behavior will result in lifting of imposed sanctions. The imposition of economic sanctions depletes the negative consequences that an indicted actor could expect to suffer from committing recidivist cyberattacks. Under the cost-benefit calculus, the imposition of economic sanctions undermines the specific deterrent effect of bare indictments because imposing economic sanctions lowers the expected cost of recidivist cyberattacks.

///

///

6.3.4. Imposition of Economic Sanctions Would Not Disrupt Business Model

The Mabna Institute case study is a clear illustration of these theoretical predictions because a disruptive effect was not present. The deterrent, as opposed to disruptive, effect can be isolated; any disruptive effect economic sanctions have upon the Mabna Institute's operations is negligible. Economic sanctions would not have been projected to disrupt the Mabna Institute's business model. The Insikt Group's 2021 report shows that the Mabna Institute's ability to circumvent economic sanctions is what largely drives the demand for its illicit hacking services. Moreover, the prediction that economic sanctions would do nothing to disrupt the Mabna Institute's operations is not a conclusion that could only have been arrived upon in hindsight with the benefit of new research findings. As shown by the press releases' assertion that the Mabna Institute was founded to "assist" Iranian academic institutions, the Mabna Institute dealt, and continues to deal, with an exclusively Iranian clientele; unless there is evidence that the Mabna Institute's finances were being run through a non-Iranian institution, blocking the Mabna Institute from dealing with U.S. persons would not disrupt its operations. Neither could the Mabna Institute's phishing tradecraft, which was known to the U.S. before the indictment was issued and the economic sanctions were imposed, be predicted to be disrupted by economic sanctions. As described in the indictment, "those spearphishing emails indicated that the sender had read an article the victim professor had recently published, and expressed an interest in several other articles. The sender provided links to those additional articles. If the victim professor clicked on certain links, he or she would be directed to a malicious Internet domain" (*Rafatnejad* indictment, 4). The success of the Mabna Institute's phishing operations – which, as the Insikt Group's report shows, continue to be conducted in much the same way

and at an accelerated pace despite the 2018 unsealing of the indictment – is not dependent on doing business with U.S. persons.

Based on the evidence that economic sanctions would have negligible disruptive effect on the Mabna Institute's operations, and based on reading Lacy's and Niou's findings to contend that imposed economic sanctions would likely not have succeeded in changing behavior at the threat stage, another counterargument may be made that the Mabna Institute would likely have been undeterred by the threat of economic sanctions, so such economic sanctions would eventually need to be imposed to sustain the U.S.'s deterrent credibility. To this potential objection, I have four responses that also serve to summarize my argument. First, the premature deployment of sanctions ruled out any likelihood – however high or low – that the Mabna Institute may have been deterred; while there was no guarantee that the bare indictment would have deterred the Mabna Institute, precluding the possibility was a guarantee that the bare indictment could *not* deter the Mabna Institute. Second, because it is the threat of economic sanctions rather than the imposition of economic sanctions that has a determinative effect on changing behavior, the deployment of economic sanctions could not be expected to enhance any deterrent effect the bare indictment may have had. Given that economic sanctions are massively costly for the U.S. to enforce, the imposition of economic sanctions when a threat may have sufficed was therefore a waste of state resources. Third, the cost was truly wasted because the imposition of sanctions could not have been predicted to engender any additional benefits of disruption. Fourth and most importantly, the cost of imposing sanctions was not only wasted but also counterproductive. By adding the Mabna Institute and its nine indicted affiliates to the SDN List, the imposition of economic sanctions engendered a binary change

in legal status – "Blocked Person" – that would be difficult to lift and could not be imposed additively. Thus, the imposition of sanctions eliminated the incentives that the Mabna Institute may have had to refrain from committing recidivist cyberattacks.

In a 1998 policy brief, diplomat Richard N. Haass called attention to economic sanctions' lack of specific deterrent effect and argued that a tailored rather than one-size-fits-all approach would better serve the U.S.'s policy goals: "all too often sanctions turn out to be little more than expressions of U.S. preferences that hurt American economic interests without changing the target's behavior for the better. As a rule, sanctions need to be less unilateral and more focused on the problem at hand" (Haass 1998). If economic sanctions are "little more than expressions of U.S. preferences," they are partially duplicative of the effect of bare indictments. If norm-setting against cyberattacks to achieve general deterrence was the intention, bare indictments will often be sufficient; there is no need to incur the cost of sanctions enforcement. I have used the Mabna Institute case study to argue that, where a deterrent effect could already have been achieved by the bare indictment, economic sanctions should not be blindly imposed in tandem; doing so in the name of consistency may not only be a wasted cost, but also undermine the deterrent effect.

Following Peters' and MacConaghy's call for critical assessment of cyber sanctions' impact, the Mabna Institute case study can serve as an example where economic sanctions against alleged cyberattackers did *not* achieve the U.S.' policy goals because the deployment of economic sanctions was premature, unnecessary, and counterproductive. To ensure that strategic missteps do not render the deterrent effect suboptimal, I suggest that practitioners be mindful that the binary structure of economic sanctions against

specific actors can deplete the incentive for these actors to refrain from continuing to commit cyberattacks.

6.4. Chapter Conclusion: Enhancement and Interference

Examining these two counterexample case studies, each of which contradict the predictions of the theory, has yielded further insights on how actual apprehensions can enhance the deterrent effect of bare indictments and why the imposition of duplicative economic sanctions can interfere with the deterrent effect of bare indictments.

An underlying, often overlooked feature of bare indictments is that they do facilitate legal apprehension, upon which point the informal sanctions associated with apprehension are imposed and formal legal consequences can be expected to result. Although Hinck and Maurer argue that very few bare indictments of actors who can be linked to the nation-state have led to arrests (2020, 527), it is important to recognize that the risk of apprehension, and the risk that formal legal consequences will apply, underlie all bare indictments. In the Arrow Tech case study, these risks were made even more contemplable by the arrest and conviction of a co-conspirator; although the motive of Ajily and Rezakhah was ambiguous, bare indictments' raising of their expected weighted cost served as a deterrent measure that operates irrespective of motive.

In this chapter, I also used the March 23, 2018 unsealing of a bare indictment against affiliates of the Iran-based Mabna Institute to argue against scholars who posit that economic sanctions should always be imposed in tandem with bare indictments against cyberattackers. I drew upon the principles of CDT and the literature on economic sanctions to show that imposition of economic sanctions against indicted cyberattackers can

counterproductively undermine the deterrent effect; economic sanctions should not be simultaneously imposed as a matter of policy. Thus, understanding the mechanistic features of bare indictments generates practical recommendations such as those that will be further discussed in the next chapter.

CHAPTER 7

LEVERAGING BARE INDICTMENTS:

IMPLICATIONS FOR POLICY AND RECOMMENDATIONS FOR PRACTITIONERS

7.0. Chapter Overview: Policy Implications and Recommendations

This chapter regards the theory's policy implications; I use these implications to provide recommendations for practitioners and for policy advocates. A consolidated summary of these recommendations in bullet-point format may be found in Section 7.8.

Sections 7.1. through 7.7. discuss those practical recommendations in detail. Section 7.1. starts from the broad suggestion that § 1030 bare indictments should be issued and publicized whenever possible; § 1030 bare indictments are especially likely to achieve specific and general deterrence when the cyberattacks are motivated by status-seeking or thrill-seeking, but my study has shown that alternative mechanisms of deterrence mean that § 1030 bare indictments can also deter irrespective of cyberattacker motive. In Section 7.1., I address the counterargument that bare indictments' revelation of sources and methods makes them unsuitable for use as a deterrent measure. I examine American legal procedure to show why the premises upon which this counterargument is based are faulty. I also argue that bare indictments can be seen as an optimally efficient deterrent measure against cyberattacks; the capacity to bluff using bare indictments makes their likelihood of remaining 'bare' a boon, not a detriment.

Section 7.2. discusses the advantages and disadvantages of using conspiracy charges and criminal complaints to accomplish similar functions as would a § 1030 bare indictment. In Section 7.3., I give a list of guidelines for assessing whether imposing

economic sanctions in conjunction with a § 1030 indictment is counterproductive of deterrence. Section 7.4. revisits the SamSam Ransomware case to give an example of other policy objectives that can be achieved by simultaneous imposition of economic sanctions. Section 7.5. discusses in more detail the possibilities for leverage of CMAAs to enable apprehensions in non-extradition countries. Section 7.6. explores how informal sanctions can be triggered pursuant to the criminal procedures of other jurisdictions. In Section 7.7., I recount some policy trends and review the most relevant suggestions for policy advocacy.

7.1. Practical, Legal, and Ethical Use of Bare Indictments as an Efficient "Bluff"

This section draws from the PLA Unit 61398 case study to discuss policy implications on the practical, legal, and ethical use of bare indictments as an efficient deterrent measure that achieves general norm-setting against status-seeking cyberattacks. As a starting point, I address some scholars' counterargument that bare indictments are, on balance, too costly for the U.S. to use as a deterrent measure because deploying them may lead to the U.S.'s being required to disclose and hence compromise its sensitive sources and methods. Examining how bare indictments fit into American legal procedure shows that the issuer of a bare indictment can almost always "bluff" and only under comparatively unlikely circumstances be required to follow through on the arrest of the indicted defendants. I also discuss why American legal ethics rules constrain practitioners from making empty bluffs. Overall, this section argues that bare indictments are an optimally efficient deterrent measure against cyberattacks not only because – as shown by the case studies – bare indictments can achieve specific and general deterrent effects, but also because they can often achieve such effects without the issuer having to follow through on

the costly and time-consuming process of imposing formal legal punishment. It should be seen as a boon, not a detriment, when a bare indictment achieves deterrent effects yet can remain "bare."

Whenever there is enough evidence to compile an indictment, bare indictments should be issued and publicly announced to serve as a deterrent measure against cyberattacks. This recommendation applies irrespective of motive; in Chapter 5 and Chapter 6, I explored alternate ways that bare indictments can deter cyberattacks by attacking national face or by imposing a contemplable risk of apprehension. However, the specific and general deterrent effects seem to be particularly strong when evidence indicates that the individuals to be indicted are status-seeking. As the PLA Unit 61398 case study illustrates, bare indictments can achieve measurable and dramatic deterrent effects against prestige-seeking cyberattackers, even when the cyberattackers are apparently backed by a nation-state.

Compromising sources and methods – a risk some scholars have theorized (Hinck and Maurer 2019; Machtiger, April 03, 2020; Machtiger, October 29, 2020; Pruitt 2021) – should not impede bare indictments' use as a deterrent measure, since an examination of U.S. legal procedure indicates that this would only be a risk if the indictment were improperly prepared. An example of the argument that bare indictments risk revealing sources and methods comes in Ellen Pruitt's 2021 article for the *University of Baltimore Law Review*. Citing to Hinck's and Maurer's 2019 piece for *Lawfare*, Pruitt writes, "Because the indictments lay out the entire investigation and case of the prosecution, they typically

include national security details. These national security details tell adversaries in no uncertain terms how the U.S. is obtaining the information on the cyber actors" (2021).

I argue that these premises are faulty. Hinck's and Maurer's 2019 piece discusses "revealing U.S. intelligence sources and methods" as a risk of *criminal charges* generally, not *indictments* specifically. Under U.S. law, another type of federal criminal charges – distinct from indictment – is a criminal complaint. An affidavit to support a federal criminal complaint under U.S. law typically could, in a milder version of Pruitt's assertion, lay out *some* details about the investigation's sources and methods (see *Su Bin* criminal complaint). By contrast, U.S. federal criminal indictments normally do not discuss sources and methods used in the investigation. Indeed, an indictment that included sources and methods would likely be regarded by most American legal practitioners as ridiculously poorly written, since such an indictment includes too much extraneous material that is confusing at best and harmful to the prosecution's own case at worst.

Unlike the 2013 Mandiant report, nowhere in the indictment against the five PLA Unit 61398 officers did the written text go into detail as to how the information was obtained. An example is line item 16 of the *Wang Dong* indictment, where the indictment listed several domain names that the PLA Unit 61398 officers had allegedly used, but did not discuss how it was determined that the defendants had used these domain names (*Wang Dong* indictment, 11-12). It was a private company's technical attribution report, not the U.S. federal government's indictment, that would have already revealed details about technical attribution sources and methods. Unless an indictment is written flagrantly out of conformity with basic standards in U.S. criminal law practice, indictments certainly

do not, as Pruitt asserts, "tell adversaries in no uncertain terms how the U.S. is obtaining the information" (2021).

Neither does issuing and unsealing a properly written indictment alleging violations of 18 U.S.C. § 1030 tend to run the risk that sources and methods will be revealed by inference. Peter Machtiger's (October 29, 2020) argument that the text of indictments can "reveal clues" allowing adversaries to determine and terminate U.S. intelligence activity only cites examples to show that indictments can give adversaries generalized knowledge that the U.S. is monitoring their cyber activities. This confirmation of U.S. monitoring is not a particularly shocking or actionable revelation; as cybersecurity scholar Amy Zegart writes, the fact that "everybody spies in cyberspace" is already an assumption of most nation-state cyber adversaries (Zegart 2020). The one 'clue' that Machtiger uses as an example of how adversaries can draw inferences about the details of an investigation regards the sourcing of the photographs used to depict defendants on 'Wanted' posters (Machtiger, October 29, 2020), but 'Wanted' posters are a matter external to and separately prepared from the text of an indictment.

A variation of the argument on revealing sources is made by Goldsmith (2014); I respond by positioning this counterargument as indicative of an advantage rather than a shortcoming of bare indictments. Arguing that U.S. prosecutors would likely be required to reveal sources and methods to obtain guilty verdicts for the defendants *if the bare indictment ever resulted in a trial*, Goldsmith writes of the bare indictment in the PLA Unit 61398 case, "it seems like it would be hugely difficult to *prove* [italics in original] the charges in yesterday's indictment, consistent with the normal rules of proof in a criminal

trial, without revealing quite a lot about how the [U.S. government] spies on the Chinese government" (2014). This argument is slightly different from Pruitt's and Machtiger's arguments; rather than arguing that the text of a bare indictment reveals sources and methods, Goldsmith argues that the trial resulting from a bare indictment will require prosecutors to reveal sources and methods. I respond that this argument exposes a feature that makes bare indictments an optimal deterrent measure: bare indictments are an optimally effective deterrent measure precisely because it is expected that the bare indictment will usually remain "bare."[23] Because it is relatively unlikely that indicted foreign cyberattackers will ever voluntarily come to the U.S. to face trial, the U.S. will probably never be required to reveal its sources and methods. Since bare indictments can achieve a deterrent effect *without* necessarily revealing sources and methods, *without* necessarily incurring the cost of a trial, and *without* having to incur the cost of possibly imprisoning the defendants in the event of a guilty verdict, they are an optimally efficient deterrent measure: the U.S. has used bare indictments to achieve a deterrent effect without having to sink these costs. The issuer of a bare indictment can often expect that the issuer will never have to follow through on a bare indictment, giving the issuer a capacity to "bluff."

As a closing recommendation for this section, practitioners should not operate under a misconception that the bluff can be empty. An indictment should not and cannot,

[23] An objection to the contention that 'bare indictments can be expected to usually remain bare' would be to point to the high rate of arrests, extraditions, and convictions among the numerous Russian non-state actors indicted under § 1030; see Chapter 6. Still, it seems clear that § 1030 bare indictments usually remain bare if these Russian non-state actors are excluded. Given that some scholars and practitioners may be more interested in the deterrence of cyberattacks that arguably have nation-state backing, the premise that 'bare indictments, *other than bare indictments issued against arguable non-state actors*, usually remain bare' can be assumed.

as the Chinese state spokesperson asserted in the PLA Unit 61398 case, be "based on deliberately fabricated facts" (Qin 2020). There are at least two major reasons militating against the use of indictments as empty bluffing.

One, drawn from classical CDT, is an inefficiency issue. Bentham assumes that if a policy practitioner deliberately fabricates false charges against an innocent, the fact that a fabrication exists significantly increases the likelihood that the public will learn about the fabrication's existence (Bentham 1830, 29); the revelation of the truth, and the appurtenant revelation that an agent of the state deliberately concealed the truth from the public, will likely cause widespread outrage that outweighs the benefit of deterring the adversary (Bentham 1871, 329-330). This is directly analogical to the indicted adversary's ability to call the indicter's bluff. The reason that bare indictments are seen as "bare" is that the indicted actor is highly unlikely to be extradited to the U.S. to face trial. However, policy practitioners should be aware that there is always a chance that the indicted foreign national could call the U.S.'s bluff by 'voluntarily' coming to the U.S. to face trial even in the absence of extradition; for instance, this occurred in the Su Bin case. Bentham's theory predicts that, during a trial for a bare indictment that is "based on deliberately fabricated facts," it is highly likely that the falsity of these facts will become evident to the public. This is why policy practitioners should refrain from empty bluffing; any instance of empty bluffing carries the potential to undermine the credibility of all future bare indictments.

Two, legal ethics rules constrain the legal practitioner from using an indictment to deliberately fabricate false charges. Rule 3.3 of the Model Rules of Professional Conduct ("MRPC") issued by the American Bar Association ("ABA") – a "version of which" rule is

applicable in all U.S. jurisdictions (State Bar of California, n.d., 2) – states that "A lawyer shall not knowingly make a false statement" to a court of law (ABA MRPC Rule 3.3(a)(1)) and "shall not knowingly offer evidence that the lawyer knows to be false" (ABA MRPC Rule 3.3(a)(3)). Since bare indictments are filed with a U.S. federal court, deliberately fabricating evidence and using a bare indictment to make empty allegations would be almost indisputably a clear violation of the ABA's rule. Likewise, as Bentham predicts, the fact that actual violations have been committed makes it probable that these violations may become the basis for provoking public outrage.

Policy practitioners should realize that bare indictments can be used as bluffs that are unlikely to result in actually incurring the costs of prosecution, but should be mindful that mobilizing bare indictments as empty bluffs is arguably inefficient and unethical. On the other hand, policy practitioners can cite to the inefficiency and unethicality of fabricated indictments to bolster the bluff's credibility, showing to the public – the class of persons any of whom could be a potential cyber adversary – that bare indictments against alleged cyberattackers are not empty accusations.

As seen in the Su Bin case study, the Arrow Tech case study, and the case studies of Russian non-state actors, bare indictments can and have led to apprehensions. Thus, bare indictments cannot be empty bluffs. However, especially when an analysis of the particular case shows that it is unlikely that the U.S. will ever have to follow through with prosecuting the indicted individuals, policy practitioners should recognize it is precisely the 'bare' aspect of bare indictments that keeps the cost of specific and general deterrence relatively low, making bare indictments an optimally efficient deterrent measure.

7.2. Comparing Indictments with Criminal Complaints; Using Conspiracy Charges to Position Cyberattacks as a Global Concern

In this section, I discuss why the use of criminal complaint and the use of conspiracy charges in the Lazarus case study demonstrate further options that can be added to the practitioner's toolbox. A disadvantage of criminal complaint is that the standard of proof is weaker than in an indictment. However, lower procedural hurdles make the criminal complaint a faster track to imposing the risk of arrest. Notwithstanding that the bare indictment in the Lazarus case study could not achieve a specific deterrent effect against the profit-seeking cyberattackers, examining the procedural history and legal argumentation of this case provides an intriguing model of optimal efficiency in rallying international support. Although the criminal charges in this case are grounded in the 18 U.S.C. § 1030 unauthorized access statute, charging the individuals with conspiracy under 18 U.S.C. § 371 – charging them with *conspiracy* to commit unauthorized access, which is a charge distinct from unauthorized access itself – enabled the bare indictment to position the Lazarus Group's cyberattacks as an issue of global concern.

As the DOJ's press release in the Lazarus case study notes, related criminal charges had been issued against one of the three indicted individuals – Park Jin Hyok – in 2018 (DOJ OPA, February 17, 2021). In U.S. law, all indictments are federal criminal charges, but not all federal criminal charges are indictments. The Fifth Amendment to the U.S. Constitution requires that federal criminal prosecutions of an "infamous" crime must be initiated by an "indictment" returned by a "Grand Jury" (DOJ, January 22, 2020). In binding caselaw precedent from the U.S. Supreme Court, the term "infamous" has been interpreted to mean

crimes that are punishable than more than one year of imprisonment (DOJ, January 22, 2020). Using this definition, violations of 18 U.S.C. § 1030 often constitute violations of an "infamous" federal crime; 18 U.S.C. § 1030(c), which is the subsection that lays out the punishment for violating the statute, provides for imprisonment of up to five years for some violations, imprisonment of up to ten years for some violations, and imprisonment of up to twenty years for recidivist violations. Conspiracy under 18 U.S.C. § 371 is, likewise, an infamous federal crime; unless the "object of the conspiracy" is a "misdemeanor" – which usually means that the object of the conspiracy is a crime punishable by less than one year of imprisonment (Legal Information Institute, "Misdemeanor," 2021), and hence not an infamous federal crime – 18 U.S.C. § 371 provides that conspiracy is punishable by up to five years of imprisonment. However, if federal criminal charges are issued not to initiate a criminal prosecution, but rather, to ground an arrest warrant, then the Fifth Amendment's requirement of indictment does not apply. The federal criminal charges issued by the U.S. against Park in 2018 were to ground a warrant for Park's arrest, not to initiate a federal criminal prosecution (*Park* criminal complaint). This was an optimally efficient move on the part of the U.S. government; based on the arrest warrant, Park could be legally arrested, yet the U.S. government did not have to incur the expense of convening a grand jury in order to return an indictment that would likewise have imposed this risk of arrest upon Park.

Another optimally efficient move was charging the cyberattackers with violations of § 371. The August 2018 criminal complaint charged Park with having violated § 371, the federal conspiracy statute, by conspiring to violate § 1030 (*Park* criminal complaint). Likewise, when the grand jury returned the indictment against Park and two other North

Korean nationals who were allegedly affiliated with the Lazarus Group, the indictment charged the three individuals with having violated § 371 by conspiring to violate § 1030 (*Jon* indictment, 9). This procedural move was used to great advantage. The U.S. would not have domestic criminal jurisdiction to prosecute cyberattacks perpetrated against non-U.S. computer systems; a cyberattack perpetrated against a non-U.S. computer system would ordinarily not be a violation of § 1030. As a matter of legal strategy in charging a violation of § 1030, it would often be unwise for such an indictment to cover information focusing on cyberattacks that were perpetrated against a non-U.S. computer system, because this move would be vulnerable to the argument that the information about cyberattacks perpetrated against non-U.S. computer systems is irrelevant and therefore excludable. However, because the indictment charged the three individuals with having violated § 371, information on cyberattacks perpetrated against non-U.S. computer systems was arguably relevant; as seen in the indictment, such information could be covered as relevant "overt acts" in furtherance of the conspiracy. Indeed, many of the cyberattack-enabled heists detailed in the indictment were perpetrated against non-U.S. computer systems; for instance, "Overt Act No. 6" in furtherance of the conspiracy alleges "fraudulent wire transfers" of over 104.1 million USD from a bank in Africa "to bank accounts in Taiwan, Thailand, and Cambodia" (*Jon* indictment, 17). The indictment expressly alleges that the Lazarus Group's cyberattacks were mounted against computer systems of myriad nations including Vietnam, the Philippines, Bangladesh, Poland, and Malta (*Jon* indictment, 3). Through using the legal structure of § 371 to discuss as "overt acts" cyberattacks that were perpetrated against non-U.S. computer system, the indictment positioned the Lazarus Group's cyberatttacks as an issue of worldwide concern.

Three policy recommendations are as follows. First, if the objective is to facilitate legal apprehension of the alleged perpetrator, then practitioners operating in the U.S. federal legal system should consider pressing charges by means of a criminal complaint, since grounding a federal arrest warrant does not require convening a grand jury to return a federal indictment. That being said, a criminal complaint against an alleged cyberattacker should not necessarily replace the issuance of a bare indictment against an alleged cyberattacker. The evidentiary standard to ground an arrest warrant is based on "probable cause" (Legal Information Institute, "Probable Cause," n.d.); in layman's terms, probable cause is a relatively low standard. The information included in criminal complaints does not have to meet the higher evidentiary standard of being legally admissible at trial; by contrast, the information included in an indictment implicitly purports to be based on evidence that would be legally admissible at trial. Because the information in a criminal complaint is more disputable than the information in an indictment, a criminal complaint may not trigger the package of informal sanctions as effectively as does an indictment. In other words, an arrest warrant's lower evidentiary standard of "probable cause" means that the label of "criminal outcast" is more questionable when imposed via criminal complaint than when imposed via indictment. Thus, a criminal complaint should not necessarily be used instead of a bare indictment.

Second, neither should a criminal complaint necessarily precede a bare indictment. As mentioned, many scholars have raised concerns that any deterrent effect that bare indictments may have comes at the cost of revealing sensitive sources and investigatory methods. Although I argued in Section 7.1. that the risk of undermining future investigations is exaggerated given bare indictments' role in U.S. criminal procedure, these

concerns become more salient given the different procedural features of criminal complaints, since criminal complaints are customarily supported by an affidavit (see *Park* criminal complaint). Unlike the text of bare indictments, the text of affidavits routinely discloses details about the investigation. For instance, line item 38 in the affidavit attached to the criminal complaint against Park discusses how the investigation obtained information about a piece of malware (*Park* criminal complaint). Because affidavits do customarily include information about sources and methods whereas bare indictments do not, practitioners should not blindly deploy criminal complaints as a 'fast track' to criminal charges before convening a grand jury; rather, practitioners should consider whether the risk of undermining future investigations is justified.

Third, practitioners should learn from this case that charging a cyber adversary with conspiracy can be used to include as "overt acts" information on cyberattacks perpetrated outside of the U.S.'s domestic criminal jurisdiction. When an indictment positions the cyberattacks perpetrated by the indicted actors as a matter of global rather than solely national concern, practitioners can invoke the written text of the indictment to rally support from the international community. However, just as a criminal complaint should not necessarily replace a bare indictment, charging under § 371 should not necessarily replace charging under § 1030. This is because § 371 is only punishable by up to five years of imprisonment, whereas § 1030 can be punishable by up to twenty years. Under U.S. federal criminal law, a conspiracy charge under § 371 – *conspiracy* to commit an offense – is discrete from a charge regarding the base 'offense' that a defendant allegedly conspired to perpetrate (see *Jon* indictment, 9). Charging someone with committing an offense, such

as unauthorized access under § 1030, can stand either alone from or alongside charging someone with *conspiring* to commit that offense under § 371.

Thus, the argument could be made that the indictment against the three North Korean nationals should have charged them with violating not only § 371, but *also* § 1030; for the purposes of general deterrence norm-setting, this might have sent a clearer message that the cyberattacks themselves were offenses to be deterred. It also seems that § 1030(b) – the conspiracy subsection of § 1030 – could have been used, instead of or alongside § 371, to integrate the international 'overt acts.' It is unclear why the bare indictment did not charge the three North Korean nationals with violations of § 1030 itself; perhaps the prosecutors who prepared the indictment were more familiar and comfortable with structuring § 371 charges. Overall, I recommend that § 371 charges and criminal complaints be regarded as further options in the practitioner's toolbox, not replacements for § 1030 bare indictments.

7.3. Suggested Guidelines for Simultaneous Imposition of Economic Sanctions

Based on the discussion in the Mabna Institute case study, I suggest that practitioners should ask themselves the following questions before imposing cyber sanctions on indicted cyberattackers:

- Has a clear *threat* of economic sanctions been communicated to the actor? The answer must be yes, as actual *imposition* of sanctions incurs enforcement costs and tends not to be determinative of the deterrent effect.
- Has the actor had sufficient time or opportunity to change its behavior in response to the communicated threat of economic sanctions?

- Is the cyberattacker primarily motivated by prestige-seeking, thrill-seeking, or profit-seeking? If the cyberattacker is primarily motivated by prestige-seeking or thrill-seeking, then a bare indictment is already likely to achieve a specific deterrent effect, so imposition of cyber sanctions may be unnecessary and hence suboptimal.
- Beyond the norm-setting general deterrent effect – which may already be accomplished by bare indictment – is the imposition of economic sanctions predicted to accomplish other policy goals, such as disruption of the sanctioned actor's operations? If the imposition of economic sanctions is predicted to accomplish other policy goals beyond deterrence, imposing sanctions may be appropriate.

Policy practitioners can take the Mabna Institute case study as a cautionary example. While the Mabna Institute may have been undeterred irrespective of the U.S.'s actions, premature deployment of economic sanctions precluded the possibility of deterrence. The use of economic sanctions in conjunction with bare indictments should not jump straight to imposition, but rather, must allow the actor an opportunity to change its behavior in response to the communicated threat of sanctions. Moreover, economic sanctions should not – as some argue – be imposed against all indicted cyberattackers. Considering that the norm-setting effect of sanctions duplicates but does not augment bare indictments' general deterrent effect, the imposition of sanctions against indicted cyberattackers must be evaluated on a case-by-case basis in accordance with criteria such as those I have suggested, so as not to impede the U.S.'s own policy objectives by precluding the possibility of specific deterrence while failing to engender other policy outcomes.

This list of suggested guidelines applies if the target of the proposed imposition of economic sanctions is to be indicted or has already been indicted. As will be examined in the next section, the imposition of economic sanctions can achieve other policy objectives besides deterrence; particularly when the target of the proposed imposition of economic sanctions will *not* be subject to bare indictment, policy objectives other than deterrence may justify economic sanctions' imposition.

7.4. Other Policy Objectives when Economic Sanctions Are Not Duplicative

This section discusses the simultaneous imposition of economic sanctions upon two other individuals who were not charged in the indictment but helped facilitate the laundering of the ransoms in the SamSam Ransomware case study. I distinguish the simultaneous imposition in the SamSam Ransomware case study from the simultaneous imposition in the Mabna Institute case study. In the SamSam Ransomware case study, the economic sanctions were not duplicative because they were imposed on actors other than those who were indicted, and this imposition of economic sanctions can be projected to achieve the policy objective of disruption.

In light of the imposition of economic sanctions in the Mabna Institute, a relevant aspect of the SamSam Ransomware case bears discussion. On the same day as the DOJ's public announcement of the bare indictment's unsealing in the SamSam Ransomware case, the OFAC of the U.S. Department of the Treasury levied economic sanctions against two Iranian individuals involved with the SamSam Ransomware scheme. Usually, the public announcement of such sanctions would take the form of an "SDN List Update"; it was out of the ordinary, then, that OFAC also issued a press release. The press release called attention

to the novel move of listing the Bitcoin digital currency addresses of the two individuals: "While OFAC routinely provides identifiers for designated persons, today's action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses" (U.S. Department of the Treasury, November 28, 2018).

I used the Mabna Institute case to argue that the simultaneous imposition of economic sanctions against cyberattackers who were subject to bare indictment was suboptimal. By contrast, I would not argue that the deployment of economic sanctions against these actors was necessarily premature, notwithstanding that – as with the Mabna Institute case – the economic sanctions were imposed on the same day as the issuance of the bare indictment. What distinguishes the two cases?

The key difference is that, in the SamSam Ransomware case, the two individuals against whom sanctions were imposed – Ali Khorashadizadeh and Mohammad Ghorbaniyan – are not the same two individuals against whom the bare indictment was issued. Since the economic sanctions were not imposed against the same individuals, the imposition of economic sanctions is not duplicative of the norm-setting general deterrent effect, and CDT would not predict that the imposition of economic sanctions against Khorashadizadeh and Ghorbaniyan would undermine the specific deterrent effect of the bare indictment against Mansouri and Savandi.

Moreover, despite multiple scholars' contention that the threat of economic sanctions rather than the imposition of economic sanctions is determinative of the

deterrent effect, the imposition of sanctions may have other policy objectives besides convincing a blocked person to change its behavior. For instance, the imposition of economic sanctions may put a stop to blocked persons' operations and thereby accomplish disruption; OFAC expresses this policy objective in the second sentence quoted from the press release.

Further, Khorashadizadeh's and Ghorbaniyan's alleged role in the SamSam Ransomware scheme suggests that the imposition of sanctions could disrupt the two individuals' operations. Their role was that of currency exchanger: they would convert the Bitcoin ransoms "into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme" (U.S. Department of the Treasury, November 28, 2018). The press release goes on to imply that – unlike the Mabna Institute – Khorashadizadeh and Ghorbaniyan did conduct business with non-Iranian persons (U.S. Department of the Treasury, November 28, 2018). Thus, in addition to having a general deterrent effect on other currency exchangers who might see the negative consequences of economic sanctions imposition as a reason to avoid conducting business with cyberattackers, the imposition of economic sanctions could also be predicted to have a disruptive effect on these illicit currency conversion operations.

Relatedly, this general deterrent effect of the imposition of sanctions is not duplicative of the general deterrent effect of the bare indictment. In the bare indictment, an action that resulted in negative consequences was unauthorized access, so the bare indictment would be predicted to have a general deterrent effect against potential cyberattackers. In the imposition of economic sanctions, the action that resulted in negative consequences was converting the illicit funds procured from cyberattacks, so the

imposition of economic sanctions would be predicted to have a general deterrent effect against currency converters; it may convince them to be more mindful of indicia that funds are illicitly derived from ransomware schemes, and it may therefore convince them to refuse to conduct transactions with such funds.

Considering that the information in OFAC's November 28, 2018 press release shows that the economic sanctions were imposed on actors whose operations could be predicted to be disrupted by imposition, the imposition of economic sanctions in tandem with bare indictment in the SamSam Ransomware case may have successfully reinforced the general deterrent effect.

7.5. Leveraging CMAAs to Enable Apprehensions in Non-Extradition Countries

The Seleznev case suggests that CMAAs may be a promising means of enforcing bare indictments through enabling or requiring foreign jurisdictions' cooperation with apprehending foreign nationals. When indicted foreign nationals travel into and out of jurisdictions, the indicted foreign nationals come within the purview of Customs authorities. As of May 2022, the online list of CMAAs compiled by the U.S. DHS's Customs and Border Protection agency includes seventy-three foreign jurisdictions with which the U.S. has "signed and entered into force CMAAs" (U.S. Customs and Border Protection 2021). Of those seventy-three foreign jurisdictions, the CMAAs are legally binding upon the Customs authorities of seventy-one foreign jurisdictions – including China and Russia, two of the U.S.'s four nation-state cyber adversaries.

The circumstances of Seleznev's apprehension suggest that policy practitioners may consider looking to CMAAs as a way to increase the deterrent force of bare indictments by

backstopping them with a higher risk that the formal legal consequences will be imposed. Since the terms of each CMAA may vary, policy practitioners should be mindful to examine the particular provisions of each CMAA, and should not operate under the assumption that every CMAA will necessarily mirror the U.S-Maldives CMAA. This analysis shows that even if the Maldives as a whole continues to provide a safe harbor for Russian nationals as recently as April 2022, the U.S. could have used the U.S.-Maldives CMAA to invoke a legal obligation for the Maldivian Customs Service to cooperate with – and hence enable – the apprehension of Russian nationals.

As suggested by the above policy recommendation on leveraging CMAAs, this could mean that indicted foreign nationals not only risk arrest by traveling into jurisdictions that have an extradition treaty with the U.S., but also may risk arrest by traveling *outside their own nation at all*, if the provisions of a CMAA can be invoked. For instance, I suggest that further legal analysis may reveal that the CMAA with China or the CMAA with Russia may, if invoked, create a legal obligation for China or Russia to exercise some degree of cooperation in the apprehension of their own indicted nationals upon their transit out of the nation. This is notwithstanding the objection that many nations do not allow extradition of their own nationals; it is possible that a CMAA may be invoked not for the foreign nation to assist with the arrest itself, but rather, to establish a legal obligation for the Customs authority of one foreign nation to alert U.S. Customs as to the indicted foreign national's destination. At that point, the U.S. may be enabled to coordinate with the Customs authorities of that destination so as to extradite the indicted foreign national from that destination.

An illustrative metaphor is as follows: it is as though the call to U.S. authorities happens from the foreign national's home telephone on the foreign national's way out the door of the house. The foreign national's apprehension by U.S. authorities occurs only after the foreign national has left the house. Just as the foreign national in this metaphor was not apprehended within the house, a foreign national indicted in connection with cyberattacks would not be apprehended within the foreign national's own nation, so prohibitions on the extradition of a nation's own nationals would not apply.

Likewise, the leverage of CFAAs would not necessarily run afoul of some nations' legal prohibitions on the use of "lures." 9-15.630 of the U.S. Department of Justice's *Justice Manual* states, "A lure involves using a subterfuge to entice a criminal defendant to leave a foreign country so that he or she can be arrested in the United States, in international waters or airspace, or in a third country for subsequent extradition, expulsion, or deportation to the United States... some countries will not extradite a person to the United States if the person's presence in that country was obtained through the use of a lure or other ruse" (DOJ, April 2018). There is no evidence that Seleznev was lured to the Maldives, as he was there for a family vacation. As with the Seleznev case, it would be prudent for the respective Customs authorities of the U.S. and the foreign nation to do nothing to "entice" indicted foreign nationals to leave their home countries. Upon the invocation of a CFAA, the foreign nation's Customs authority must only stand ready to alert the U.S. Customs authority and possibly mobilize in assisting with the arrest once an indicted foreign national – of the indicted foreign national's own volition and accord – travels out of the indicted foreign national's home country or into a third country,

whichever is applicable. In such situations, there is no violation of any prohibition on the use of lures.

7.6. Using Criminal Procedure in Non-U.S. Jurisdictions to Trigger Informal Sanctions

In circumstances similar to those of the APT40 case, wherein a worldwide campaign of international cyberattacks is alleged, a policy recommendation is for each nation-state to consider formally issuing and publicizing its own domestic criminal charges, either independently or as part of coordinated international action, so as to trigger informal sanctions.

As mentioned in Chapter 3, it is remarkable that the issuance of bare indictments against suspected cyberattackers appears to be an exclusively American phenomenon, and that no other nation-states seem to have issued domestic criminal charges against foreign nation-state cyber adversaries. Perhaps a reason driving domestic criminal charges' under-leverage in other countries is the belief that bare criminal charges – because they are "bare" – cannot achieve any deterrent effect against cyberattacks. Understanding the theory on bare indictments not only can help to dispel this misconception, but also can guide the policy practitioner through navigating other nation-states' respective criminal procedures; the theory on why bare indictments deter cyberattacks makes clear that an *equivalent procedural move* that triggers the package of informal sanctions should achieve a similar deterrent effect.

In the criminal charging procedures of some national jurisdictions, the issuance of criminal charges routinely precedes apprehension. As discussed in Chapter 2, the U.S. is

one of these jurisdictions. Japan, one of the coalition members in the APT40 case, is also a jurisdiction that – like the U.S. – issues criminal charges to ground an arrest (Japanese Code of Criminal Procedure, Art. 200(1)). Jurisdictions where the issuance of criminal charges procedurally precedes apprehension should, as mentioned above, consider issuing their own domestic criminal charges against international cyberattackers; in accordance with the theory on bare indictments, doing so is predicted to deter by triggering informal sanctions that impose a contemplable risk of apprehension and label the offender a "criminal outcast."

In other national jurisdictions, however, the issuance of criminal charges is typically made *upon* arrest, following an arrest, or after the person to be charged has already been located (Crown Prosecution Service 2020, 5-7). One example of such a jurisdiction is the UK, also one of the coalition members in the APT40 case. Taking into account that the contemplable risk of apprehension and the prestige-denying label of "criminal outcast" are theorized to deter cyberattackers, policy practitioners in jurisdictions wherein charging typically occurs alongside or after apprehension might consider executing similar procedural actions that trigger these informal sanctions. To take the UK's criminal procedure as an example, those informal sanctions might be triggered when the UK's Crown Prosecution Service ("CPS") authorizes the police to charge and the UK state makes it publicly known that the police have been so authorized to charge the suspected cyberattacker. Just as offices of the U.S. DOJ issue press releases that make a bare indictment common knowledge, the appropriate governmental agencies of the UK can issue press releases to make it common knowledge that UK police have been authorized to charge the suspected cyberattacker (see London Metropolitan Police, May 26, 2022).

Analogizing from the theory on U.S. bare indictments, an equivalent governmental action in a jurisdiction such as the UK would deter by making it known to the suspected cyberattacker that there is a contemplable risk of apprehension and by making it common knowledge that the suspected cyberattacker has been labeled a "criminal outcast."

Ideally, formal criminal charges should position the cyberattacks themselves – not just behavior related to the cyberattacks – as the criminal harm to be deterred. If the domestic criminal charges concern only related behavior – such as economic espionage, money laundering, or forms of theft – at the exclusion of charging the cyberattacks, then the charges might still achieve attenuated disruptive or deterrent effects upon those accused cyberattackers, but the clarity of the message that their cyberattacks are criminal will be compromised; positioning cyberattacks as merely incidental to enable the perpetration of some other crime, rather than as harms in themselves, will be only suboptimal in advancing the setting of international norms against cyberattacks.

7.7. U.S. Government's Recognition of Bare Indictments as a Deterrent against Cyberattacks

U.S. government agencies have increasingly cited deterrence of cyberattacks as a reason for issuing bare indictments. In this section, I quote from U.S. government agency reports to evidence the trend toward acknowledging the deterrent effect of bare indictments. Relatedly, I also recount what I would present as the most important recommendations for policy advocates.

Even if there is much that remains to be understood about the mechanics of bare indictments' deterrent effect against cyberattacks, not only scholars but also U.S.

government entities have become increasingly aware that bare indictments *do* deter cyberattacks. This is evidenced by U.S. government entities' expressly positioning domestic criminal indictments as a deterrent measure. The 2020 report from the U.S. Congress' Cyberspace Solarium Commission recommends bare indictment as a norm-setting general deterrent measure in a policy of layered deterrence, stating "Law enforcement tools like criminal indictments and international extraditions contribute to layered cyber deterrence by signaling the difference between responsible and unacceptable behavior in cyberspace, thereby helping to reinforce norms" (51); the Commission positions "criminal charges (such as indictments)" as "actions designed to impose consequences and deter future malicious behavior" (108).

This understanding extends to key U.S. government officials. For instance, John Carlin – who served as U.S. Assistant Attorney General for National Security – repeatedly positioned bare indictments as an integral component in the U.S.'s cyber deterrence strategy (Carlin 2016; Viswanatha and Mann 2015; Tucker and Abdollah 2016; Lucas 2019).

Furthermore, the FBI has recently presented the indictment of Iranian cyberattackers as being in service of advancing a policy that leverages bare indictment as a deterrent measure against cyberattacks; on September 18, 2020, the FBI published an article regarding three separate § 1030 bare indictments, all three of which are discussed in Section 4.6.3. The FBI's article presented these three bare indictments against Iranian cyberattackers as "reflective of the FBI's new cyber strategy, which is to impose risk and consequences on cyber adversaries" (FBI, September 18, 2020). In addition, the FBI's article provided a link to a piece covering the "FBI's new cyber strategy." That article even

more expressly connected bare indictments to a deterrent policy, as it quoted FBI Director Christopher Wray's invocation of the potential offender's expected cost-benefit calculus: "We've got to change the cost-benefit calculus of criminals and nation-states who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves" (FBI, September 16, 2020).

Notwithstanding the lower likelihood of a specific deterrent effect being achieved by bare indictments against profit-seeking cyberattackers, policy advocates would do well to consider whether the norm-setting general deterrent effect of bare indictments may justify their imposition as an optimal deterrent measure. Policy advocates should also keep in mind that a unique feature of criminal charges is that they carry a contemplable risk of arrest; through the mechanism of imposing apprehension risk, the issuance and publicization of bare indictments can achieve specific deterrence irrespective of motive, as shown by the Arrow Tech case.

If deterrence is the policy objective, policy advocates should assess whether imposing economic sanctions will counterproductively undermine bare indictments' deterrent effect, as in the Mabna Institute case. The imposition of economic sanctions in tandem with bare indictment can be appropriate if the sanctions are imposed for a disruptive purpose, and imposition is not extraneous if the economic sanctions are imposed on persons who are connected with the cyberattacks but are not the indicted individuals.

Throughout this project, I have argued that bare indictments do achieve a general deterrent effect in changing the cost-benefit calculus of potential offenders. From the

practical standpoint of policy advocacy, what may be just as important as the validity of these theoretical and empirical contentions is the fact that bare indictments' general deterrent effect has already been *recognized* and positioned as such by entities in the U.S. government. Thus, policy advocates – whether based in the U.S. or other countries – may wish to directly cite to these U.S. government sources; positioning a policy action as being in furtherance of standing U.S. policy practice may lend it additional credence and support.

7.8. Summary of Recommendations

In summary, I suggest that practitioners and advocates operating in the legal and / or policy spheres be mindful of the following recommendations:

- So long as there is sufficient evidence to compile an indictment, § 1030 bare indictments should be issued and publicized to achieve norm-setting deterrent effects against cyberattacks. The bare indictment may be seen as an optimally efficient bluff that often achieves deterrence of cyberattacks yet rarely incurs the state costs associated with apprehension and prosecution.
- Criminal complaints are similar to bare indictments and can be a procedural fast-track to enabling apprehension. In deciding whether to prepare and file a criminal complaint, consider whether criminal complaints' procedural advantages are worth their shortcomings, such as a weaker imposition of the "criminal outcast" label and the disclosure of more details about investigatory methods.
- Conspiracy charges, such as § 371 and § 1030(b), can be used to integrate as "overt acts" international cyberattacks that would ordinarily be outside the U.S.'s

jurisdiction. Legally problematizing these international cyberattacks positions the cyberattacks as a matter of cross-national concern and can help rally support from around the globe.

- Economic sanctions should not, as some scholars suggest, always be blindly imposed in tandem with § 1030 bare indictments. Assess whether the policy objectives of imposing economic sanctions may be duplicative of, and hence counterproductive to, the deterrent effects of issuing a § 1030 bare indictment.
- Consider leveraging CMAAs to legally compel non-extradition countries to assist with apprehensions of indicted foreign nationals. Invocation of CMAAs may even legally compel non-extradition countries to assist in the apprehensions of the countries' own nationals.
- To strengthen deterrent norms, non-U.S. jurisdictions should issue and publicize their own domestic criminal charges against cyberattacks. In jurisdictions wherein apprehension typically precedes the issuance of criminal charges, practitioners should execute an equivalent procedural action to trigger informal sanctions.
- When advocating for the use of bare indictments, domestic criminal charges, or other equivalent procedural actions as a deterrent measure against international cyberattacks, consider citing to the U.S. government's written sources; position bare indictments' deterrent effects as a matter of recognized, tried-and-true policy practice.

CHAPTER 8

FURTHER APPLICATIONS OF THE THEORY:

USING BARE INDICTMENTS TO DETER AND DE-ESCALATE CYBER WARFARE

8.0. Chapter Overview: Does the Theory Hold against Cyber Warfare?

Two research questions form the impetus for this chapter: Why else does understanding the deterrent effect of bare indictments matter? What further applications does the theory on bare indictments have?

Rather than leave these questions only partially answered, this chapter discusses a further application that serves as a culmination of the insights generated from the preceding case studies: using bare indictments to deter cyberattacks even when such cyberattacks arguably amount to actions of cyber warfare.

Although I would argue that this extrapolation straightforwardly builds upon rather than contradicts the bare indictment mechanisms that this project has discussed, the extrapolation may initially seem non-intuitive due to this project's leverage of the principles of *criminal* deterrence theory rather than of *state* deterrence theory. This project has already shown evidence to contend that bare indictments can deter nation-state actors and nation-states themselves; nevertheless, at first glance, it may seem infeasible that bare indictments can deter actors who are so highly motivated that they use cyber means not just to facilitate a taking of data, but further, to cause destruction that renders inoperable those myriad quotidian tasks that are connected to the digital world. In subsection 2.2.1., when discussing the definition of a cyberattack, I suggested that a deterrence study that made use of a broad definition of "cyberattack" based on the action

itself, rather than a narrow definition based on the amount of damage caused, would generate insights that are more broadly applicable and adaptable. I analogized this to why aiming to deter the action of "theft," rather than only the taking of items of sufficient monetary value to meet the metric of "grand theft," can speak to the deterrence of petty theft and grand theft alike. Accordingly, to provide evidence that bare indictments deter cyberattacks irrespective of the extent of damage caused, I aim to once again demonstrate why bare indictments deter "cyberattacks" – even those cyberattacks that can be fairly described as acts of cyber war.

I so demonstrate by focusing on two case studies. The first case, involving a bare indictment publicly unsealed on March 24, 2016 for cyberattacks against U.S. financial institutions, shows how positioning cyberattacks as a domestic criminal matter rather than a matter of international law can serve as a de-escalatory response that deters cyberwarfare. In this case study, I engage with a psychological framework of humiliation to show why bare indictment served as an optimally effective deterrent measure. I also raise the importance of "legitimacy" under the international laws of war in order to show why the issuance and publicization of a bare indictment were legally and ethically licit; relatedly, I discuss why bare indictments' legitimacy contributes to their practical effectiveness in achieving de-escalation.

The examination of bare indictment as a de-escalatory measure in cyber warfare speaks to how the insights yielded from this project can inform recommendations for the international community's next actions in response to Russia's military invasion of Ukraine in late February 2022. Alongside this military invasion came cyberattacks against Ukrainian computer systems; the utilization of traditional armies alongside cyberwar

makes Russia's invasion of Ukraine characterizable as "hybrid warfare." I review analyses of the Russian state's arguably nationalistic motives to show why domestic criminal indictments are likely to achieve a deterrent effect even in such circumstances of hybrid warfare. By denying the objective of status and reaffirming the issuer's state sovereignty, domestic criminal charges directly frustrate an adversary's nationalistic dominance-seeking motives; I draw from previous case studies to explore the implications of this policy recommendation and its interaction with the SDT concept of "extended deterrence." This second case study, then, draws from previous case studies to support in-depth suggestions for setting global norms that can achieve a general deterrent effect against future status-seeking cyber conflicts.

8.1.0. Bare Indictment as a De-Escalatory Response to Avert Cyberwar [IRAN-02]

On March 24, 2016, the DOJ's Office of Public Affairs and the U.S. Attorney's Office ("USAO") for the Southern District of New York ("SDNY") each issued press releases announcing the indictment of seven Iranian nation-state actors who had allegedly mounted widespread distributed denial of service ("DDoS") attacks that crippled U.S. financial institutions. This indictment, apparently the first 18 U.S.C. § 1030 indictment to be levied against Iranian state actors, is another example of the effectiveness of bare indictments against prestige-seeking cyberattackers. In this case, the deterrent effect is particularly remarkable when juxtaposed against an alternate course of action that the U.S. justifiably might have taken, considering that the circumstances of these cyberattacks fall squarely within definitions of cyberwarfare. The cyberattacks, which were attributed to the Iranian state, could have been considered acts of war justifying a retaliatory response in kind from

the U.S. Instead, by situating the U.S.'s response within the criminal dimension of these attacks, the bare indictment not only frustrated the Iranian state's goals in initiating this conflict, but also transformed what could have been a full-blown cyberwar into a cyberwar that never came to pass. Therefore, the cyber indictment publicly announced on March 24, 2016 is remarkable in its provision of a case study for how bare indictments may be leveraged for averting future cyberwars.

In this case study, I first – as with the preceding case studies – analyze the circumstances of the cyberattacks to determine the perpetrators' likely motive; the temporal circumstances of the case and the nature of the cyberattacks clearly indicate that the motive was primarily prestige-seeking. Then, I review definitions of cyberwar and cyberwarfare in order to show that the DDoS attacks attributed to the Iranian state may be considered an act of war. I next examine what was achieved by the U.S.'s responding through domestic criminal charges notwithstanding that counterattacking the Iranian state was arguably justified. I engage with a psychological framework of humiliation to explicate why the U.S.'s framing the cyberattacks as a domestic criminal matter rather than treating them as acts of international cyberwar denied the Iranian state its objective of prestige yet also de-escalated the conflict. This section closes with reflections on how the outcomes of this case may be generalized to inform further harnessing of the bare indictment mechanism as a de-escalatory response to defuse cyber conflict even when such conflict amounts to cyber warfare.

///

///

8.1.1. DDoS Attacks Indicate Dominance-Seeking Motives

The text of the indictment indicates that the criminal charges were issued against seven individuals for allegedly waging a coordinated campaign of cyberattacks starting in December 2011 and peaking in September 2012 (*Fathi* indictment, line item 8). The indictment collectively termed these cyberattacks the "U.S. Financial Industry DDoS Attacks" (*Fathi* indictment, line item 7). The indictment alleged that these individuals waged the U.S. Financial Industry DDoS Attacks on behalf of the Iranian state; the indictment described the seven individuals as private contractors who had been hired by the Islamic Revolutionary Guard Corps ("IRGC"), an intelligence agency of the Iranian government (*Fathi* indictment, 1). The cyberattacks in question targeted federally protected U.S. financial institutions such as American Express, J.P. Morgan, Ally, Bank of America, Capital One, U.S. Bank, Wells Fargo, and the New York Stock Exchange (*Fathi* indictment, 5). The DDoS attacks operated via overloading these financial institutions' servers, disabling them and rendering them inaccessible by users (*Fathi* indictment, 2-4). Since these servers were used exclusively by the financial institutions (*Fathi* indictment, 9), the seven individuals were charged under 18 U.S.C. § 1030(a)(5)(A), regarding "knowingly [causing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally [causing] damage without authorization, to a protected computer." Moreover, one of the individuals was also charged under 18 U.S.C. § 1030(a)(5)(B) – "intentionally [accessing] a protected computer without authorization, and as a result of such conduct, recklessly [causing] damage" – as the indictment alleged that this individual had hacked into the control system of the Bowman Dam in Rye Brook, New York and obtained data that would have allowed the individual to take control of the dam,

but for a maintenance issue that coincidentally prevented the individual from so doing (*Fathi* indictment, 14-16).

Based on the information contained in the indictment and on the surrounding circumstances of the cyberattacks, it appears that these cyberattacks were primarily motivated by dominance-seeking. Although the DDoS cyberattacks were mounted against financial institutions, there was no data theft or currency theft alleged. Therefore, it is unlikely that profit-seeking played any part in motivating the cyberattacks, much less was the primary motivation. Furthermore, the attribution to the Iranian state – when coupled with the proximity in time to a U.S. action that threatened the Iranian state's face – evidences the contention that the Iranian state was motivated by regaining lost status. According to the Council for Foreign Relations' report, retaliation likely motivated the DDoS attacks: "At the time [circa September 2012], the media reported that U.S. intelligence believed that the denial of service was in response to U.S. imposed economic sanctions to counter Iran's nuclear program" (Council on Foreign Relations, n.d.). The dominance-seeking in this case arguably surpassed the domestic criminal dimension and entered the domain of cyberwar.

8.1.2. Dominance-Seeking Motives for Acts of Cyber War

At the time of the indictment's unsealing as well as in hindsight, the U.S. Financial Industry DDoS attacks and the unauthorized access to the Bowman Dam's control system were framed as having alarming implications for international cyberwarfare. The March 24, 2016 press release issued by the USAO SDNY included a statement from Manhattan U.S. Attorney Preet Bharara, in which Bharara highlighted that the cyberattacks had caused

widespread damage to noncombatant targets (see Arneson 2006), having "resulted in hundreds of thousands of customers being unable to access their accounts and tens of millions of dollars being spent by the companies trying to stay online through these attacks" (USAO SDNY, March 24, 2016). Bharara also called attention to the attributed state sponsorship and cross-territorial nature of the attacks: "The infiltration of the Bowman Avenue dam represents a frightening new frontier in cybercrime. These were no ordinary crimes, but calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people. We now live in a world where devastating attacks on our financial system, our infrastructure, and our way of life can be launched from anywhere in the world, with a click of a mouse" (USAO SDNY, March 24, 2016).

In an article published July 2013 – after the September 2012 peak of the U.S. Financial Industry DDoS Attacks, but years before the March 2016 unsealing of the indictment – cyber practitioner Emilio Iasiello discussed the U.S. Financial Industry DDoS attacks in the context of arguing that "there is no cyber equivalent to nuclear deterrence" (Iasiello 2013 at sec. 2.). At the time of Iasiello's writing, U.S. officials suspected Iranian state involvement, but the cyberattacks had not yet been formally attributed to the Iranian state, and credit for the cyberattacks had been claimed by a group not affiliated with the seven individuals who were eventually charged (Iasiello 2013 at subsec. 3.C.). Iasiello framed the September 2012 cyberattacks as a possible "retaliatory strike" by the Iranian government in response for the continuing U.S. economic sanctions and called attention to U.S. government officials' growing concern that cyberattacks could be used to disable U.S. critical infrastructure (Iasiello 2013 at subsec. 3.C.). Writing in August 2019, technology

reporter Andy Greenberg included these cyberattacks in an article on the history of cyberwar (Greenberg 2019), quoting the definition proposed by Richard Clarke and Robert Knake (2010): "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption."

Indeed, despite continuing scholarly debate over the precise definitions of "cyberwar" and "cyberwarfare," it seems that the cyberattacks described in the indictment fall squarely within acts of cyberwarfare, and possibly acts of cyberwar. As Greenberg analyzed, "Put more simply, [Clarke's and Knake's] definition roughly encompasses the same things we've always identified as 'acts of war,' only now carried out by digital means" (2019). Similarly, the definition currently used by the RAND Corporation involves a nation-state mounting a cyberattack against another nation-state with the intent to cause damage, and the definition specifically mentions DDoS attacks as an example: "Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks" (RAND Corporation 2021). The cyberattacks described in the indictment clearly meet every element of this definition, since they were allegedly perpetrated by the Iranian state and aimed to damage the U.S. financial institutions. From the perspective of a broader, law-based definition, the cyberattacks are even more obviously characterizable as cyberwarfare. In the introduction to a 2015 edited volume entitled *Cyber Warfare: A multidisciplinary analysis*, international law scholar James A. Green draws a distinction between "cyber war," which may connote engagement in a conflict; and cyber warfare, which includes "warlike" acts of aggression between nation-states (Green 2015a, 1-2). One could say, therefore, that the Iranian state-

sponsored cyberattacks were clearly cyberwarfare. Although it could have been argued that the real initiator of the conflict was the U.S., the U.S. imposition of economic sanctions – seemingly the basis for what Iasiello characterized as Iran's 'retaliatory strike' – had no aim to cause damage, and therefore is not an act of cyberwarfare. Thus, the cyberattacks attributed to the Iranian state would likely qualify as "acts of war," with Iran as the initiator of a cyber conflict against the U.S.

8.1.3. The U.S. Could Have Escalated The Conflict

Under the principles of the *ius ad bellum*, or the international law principles regarding when it is licit to use force in entering a conflict, the U.S. would arguably have been justified in defensively using cyber force in kind against Iran (see Green 2015b; Aiesi and Minikus 2020). The U.S. had not only arguable legitimacy, but also willingness, capability, and strategic rationale on its side. Iasiello's 2013 article references a November 2012 news report from the *Washington Post*, stating that U.S. President Barack Obama had signed in October 2012 Presidential Policy Directive 20, "a secret directive that effectively enables the military to act more aggressively to thwart cyber-attacks on the nation's web of government and private computer networks" (Nakashima, November 14, 2012). Thus, very shortly after the September 2012 cyberattacks, the procedural and bureaucratic path was prepared for the U.S. military to respond with force to the cyberattacks. Moreover, a leaked Presidential Policy Directive also issued in October 2012 and later obtained by the *Washington Post* urged the U.S. to further develop "destructive cyberwarfare capabilities that could be triggered… against adversaries around the world" (O'Harrow and Gellman 2013). The technological ease of executing a DDoS attack means that it is highly unlikely

the U.S. would have lacked second-strike capability to respond with its own cyberattacks (see Cloudflare, "How to DDoS," n.d.), and the leaked Directives evidence that there was the political will to mount such a response. The close temporal proximity between the September 2012 cyberattacks on U.S. financial institutions and the October 2012 presidential directives authorizing military action against cyberattacks suggests that the two directives were specifically prompted by concern over those cyberattacks and over how like cyberattacks could be addressed.

With the cyberattacks as a 'first strike' already having been executed by an adversary thought to be Iran, the escalatory logic of MAD in NDT would – it may be argued – also have predicted that the aggressive cyber actions attributed to Iran would escalate *unless* the U.S. were to respond to Iran with force in kind. Doing otherwise, such as not responding with proportional escalation or not responding at all, would undermine the U.S.'s credibility and therefore instill in adversaries the perception that the U.S. was a vulnerable target for further cyberattacks (see Straub 2019; Powell 1989; Zagare and Kilgour 1998; Kydd 1997; Glaser 1992).

8.1.4. The Label of Criminality as Humiliation and De-Escalation

Yet, as a consequence of the U.S.'s response via bare indictment rather than use of force, what could have been a destructive cyberwar never came to pass. I suggest that by positioning the U.S. Financial Industry DDoS attacks and the unauthorized access to critical infrastructure as domestic criminal matters rather than acts of cyberwar, the U.S. not only deterred the perpetrators via lowering expected benefit, but also achieved strategic goals such as instilling humiliation and maintaining ethical efficiency. Since the deterrent effect

and these advantages were achieved at relatively low cost, this case study serves as an example of bare indictments as optimal deterrence.

Assuming – as was discussed above – that the cyberattackers' motive was dominance, the theoretical path for the bare indictment mechanism to achieve deterrence in this case is by lowering the expected benefit of status. The information in the indictment and the circumstances surrounding the cyberattack support an argument that the cyberattackers were seeking status via dominance. Triggering the package of informal sanctions labels the cyberattacks' perpetrators as criminal outcasts, communicating that the cyberattacks failed to garner the desired objective of status. CDT predicts that, as a consequence, it was also likely communicated to the perpetrators that 'recidivist offenses' of further cyberattacks would also fail to establish dominance. In accordance with the theoretical predictions of CDT, and especially in contrast to NDT's predictions of escalation if the U.S. were not to counterattack, it appears that the bare indictment achieved a deterrent effect via lowering expected benefit. The deterrent effect is particularly remarkable considering that many conditions pointed to the onset of full-scale cyberwar.

Another noteworthy aspect that may be highlighted about this case is that the bare indictment mechanism of domestic criminal law enabled the U.S. to deny Iran's claim to status, yet this public humiliation did not anger Iran and hence provoke further attacks. The process can be explained by reference to Walter J. Torres' and Raymond M. Bergner's psychological framework of humiliation (2010). According to Torres and Bergner, humiliation involves four components; the first two are most pertinent to this case. One, there must be an attempt by the claimant to claim status (Torres and Bergner 2010, 197). Two, the status claim publicly fails; if the status claim fails in private, the claimant

experiences "painful self-realization" rather than humiliation (Torres and Bergner 2010, 197). Three, the "degrader" – the person imparting the humiliation – must be seen as having the high status necessary to humiliate the other (Torres and Bergner 2010, 197-198). Four, the claimant's low status is affirmed: "the very status of the claimant to make such a status bid or claim is rejected… the individual is branded a pretender, someone who had no business making the status claim to begin with" (Torres and Bergner 2010, 198).

The case at hand fits within this framework of humiliation. For the first component, as was discussed above, Iran was the claimant of status; dominance-seeking involves a claim to high status in relation to others. The informal sanction of being labeled a criminal outcast meant that the public announcement of the bare indictment's unsealing marked the public failure of Iran's status claim; indeed, Torres and Bergner specifically discuss the label of "criminal" as a marker of low status, an example of "stigmatized positions in society" (2010, 199). As for the third and fourth components, the U.S.'s denial of Iran's claim to status implicitly cements the status hierarchy. The act of humiliation is necessarily something that can only be executed by a high-status actor to an already low-status actor, ergo an act of humiliation serves as an implicit communicative affirmation of the actors' respective ranks in the relevant social hierarchy.

Why, then, was Iran not angered and provoked into mounting further escalatory cyberattacks? Torres' and Bergner's discussion of the consequences of humiliation provides a clue: "Understandably, the anger provoked by being severely publicly humiliated, *particularly when the humiliation is experienced as unjust and undeserved* [emphasis added], can be extreme" (2010, 200). This indicates that although anger may follow as a consequence of humiliation even if there is no concomitant experience of

injustice, it is less likely that anger will follow as a consequence of humiliation if there is no concomitant experience of injustice. Indictments, such as the bare indictment in this case, are based on factual evidence. There was therefore little reasonable basis for any actor – whether Iran or another member of the global audience – to perceive the extent of the humiliation as "unjust and undeserved"; the U.S.'s act of humiliation was not imposed arbitrarily, but rather, was factually based and was grounded in the criminal harms that had been committed. Because there was little basis to view the bare indictment, an act of humiliation, as "unjust and undeserved," it was relatively unlikely that Iran would have been angered to the extent necessary to provoke further cyberattacks. This case hence illustrates why the bare indictment mechanism can humiliate adversaries without tending to anger them to the point that they are provoked into escalating the situation.

8.1.5. Bare Indictments as an Optimal Deterrent Measure against Acts of Cyber War

The act of humiliation's being positioned as a matter of domestic criminal law connects to a second achievement of the bare indictment mechanism: ethical efficiency. Specifically, the bare indictment achieved de-escalation while dealing solely with issues of domestic law, and *without* having to engage with more contestable principles of international law. Above, I argued in brief form that the September 2012 cyberattacks – if attributable to the Iranian state as described in the indictment – against financial institutions could have been considered acts of war against noncombatant targets and that the U.S. would therefore have been justified in responding with second-strike cyberattacks. Despite the arguments I have laid out, it is frequently debatable whether a given action is justified under the laws of war (see Aiesi and Minikus 2020). Moreover, the legitimacy and

applicability of the laws of war are themselves contested (Wolfrum 2011; Thomas 2014), particularly so when considering how they might apply to damage-causing acts in the cyber arena (Green 2015b). Even if the ethical issues over whether the laws of war ought to be abided by are completely set aside, the practical reality is that establishing the U.S.'s compliance with the laws of war in matters of cybersecurity would have been bureaucratically fraught. Presidential Policy Directive 20, one of the two directives issued in October 2012, specifically dictated a procedure to ensure that any use of cyber force would comply with laws of war: "The policy also lays out a process to... ensure that... international laws of war are followed" (Nakashima, November 14, 2012). If – as I have argued – the bare indictment did achieve a deterrent effect, then it did so with relatively little cost expended. If the U.S. had endeavored to use cyber force as a deterrent, then the U.S. would have been required to grapple with whether use of cyber force was, in the abstract, justified under the contested principles of *ius in bellum*; and to navigate the bureaucratic process in place for procedurally so ensuring. By choosing to respond via bare indictment and deciding not to counterattack with use of cyber force, the U.S. was able to deter Iran from further acts of cyberwarfare. Because the strategic path taken to mount a deterrent response was the simpler one of domestic criminal law rather than the more complex route involving international laws of war, the U.S. avoided the thorny legal issues and bureaucratic requirements that would have been invoked by needing to justify use of cyber force. Since it was a lower-cost path to achieving a deterrent effect, the U.S.'s bare indictment in response to what were arguably acts of cyberwarfare perpetrated by the Iranian state was ethically efficient.

Thus, this case study of the U.S.'s bare indictment against cyberattacks attributed to the Iranian state yields at least three major insights. One, the deterrent effect of bare indictments is particularly significant in this case because bare indictment appears to have deterred the onset of full-scale cyberwarfare. Cyberwar with Iran was far more than a remote possibility. If the U.S. had responded in accordance with NDT and mounted cyberattacks against Iran as a deterrent measure – a move that NDT game-theoretic models posit would be required to maintain credibility – then NDT would also predict that the situation would escalate. Two, analysis of this case explicates why bare indictment deterred without escalation. Humiliation directly frustrates prestige-seeking, and when there is little basis to believe that an act of humiliation is unjust, humiliation is unlikely to provoke anger. Three, the bare indictment's justification under domestic criminal law rather than international laws of war makes it a relatively low-cost deterrent measure, and therefore a model for optimal deterrence.

8.1.6. Bare Indictments Are Justifiable under International Laws of War

Relatedly, these insights speak to the use of bare indictments in foreign policy. The existence of domestic bare indictments as a deterrent measure may have implications for the international laws of war as applied to cyberattacks: issuing a domestic criminal indictment could come to be considered a prerequisite for use of cyber force. Under the *ius ad bellum*, "necessity" is required; according to Matthew J. Aiesi and Amanda L. Minikus, "'Necessity' predicates any use of force in self-defense under *jus ad bellum* and means that no reasonable alternative means of redress are available to the victim state – including diplomatic efforts, which must be exhausted or deemed fruitless in stopping an armed

attack" (2020). Aiesi and Minikus provide an example of how diplomatic communication could be used to establish necessity; "the United States may implicate the *jus ad bellum* framework by simply and explicitly warning Iran that it views certain actions as illegal 'uses of force' or 'armed attacks' that would, in the U.S. view, trigger its right to self-defense under Article 51 of the U.N. Charter" (2020). If, however, it is argued that bare indictments' deterrent effect qualifies them as a 'reasonable alternative means of redress,' then it could also be argued that the necessity principle in *ius ad bellum* would require that bare indictments would have to be issued, i.e. 'exhausted or deemed fruitless,' against state-sponsored cyberattacks even before a diplomatic communication threatening exercise of the right to self-defense in the cyber arena is issued. The prerequisite of using bare indictments to deter cyberattacks resonates with James A. Green's suggestion that the principle of necessity under the *ius ad bellum* may to require states to establish that they have satisfied the "duty to prevent" cyberattacks that could be construed as acts of cyberwarfare (Green 2015b, 116).

By being a legally streamlined and procedurally straightforward path to deterrence, bare indictment – a state action grounded in domestic criminal law – is also a fast track to legitimacy. Aiesi and Minikus discuss why the success of deterrent measures – specifically, deterrent measures taken against Iran – is a function of both ethical actuality and practical perception: "U.S. military doctrine acknowledges that 'legitimacy,' which is rooted in 'the actual and perceived legality, morality, and rightness of the actions from the various perspectives of interested audiences,' is a decisive factor in military operations. If one side to a conflict establishes clear legal justification for its actions first, labeling those actions as legitimate becomes much easier for the international community. Conversely, it is rare that

illegal actions are perceived as legitimate" (Aiesi and Minikus 2020). *Actual* legal justification, hence, is almost always followed by *perceived* international legitimacy. In accordance with the jurisprudential principles of CDT, a bare indictment against an arguable act of cyberwarfare is grounded in domestic criminal law by the state's constitutive function in protecting its own inhabitants from harm. Moreover, it can be relatively straightforward to establish the domestic legal justification for state action; so long as a domestic criminal law such as 18 U.S.C. § 1030 is codified by statute, domestic statutory law can be cited in place of the more nebulous principles of international laws of war. Legitimacy appears to have been achieved via bare indictment in this case; had the U.S. engaged in cyberwar with Iran, the U.S. would likely have been subject to increased scrutiny and criticism from the international community, whereas the U.S.'s justifying its action under domestic criminal law minimized any basis the international community would otherwise have had for critique.

A final implication for bare indictments' use in foreign policy is that bare indictments would be very difficult for any other member of the global community to contest or otherwise oppose. According to Green, a principle of customary international law is "the principle of non-intervention": as has been established by declaration of the United Nations on the subject of "sovereignty," "one state cannot intervene in the domestic affairs of another state, so as to coerce it to act in a certain way" (Green 2015b, 108). Since bare indictments against cyberattacks are wholly grounded in domestic criminal law, they would qualify as domestic matters, rendering them almost uncontestable on an international basis. When a state issues a bare indictment of a cyberattack, bare indictments' grounding in domestic criminal law renders them legitimate such that any

action taken against them by another state would likely be deemed actually illegitimate and therefore denounced from the viewpoint of other members of the international order.

8.1.7. The Effectiveness and Legality of Bare Indictments as De-Escalatory Measures

In conclusion, the case study of the bare indictment issued by the U.S. on March 24, 2016 against seven Iranian individuals alleged to be state-sponsored cyberattackers explicates crucial features of the bare indictment mechanism in de-escalating cyber conflict. The bare indictment was an effective deterrent measure for averting cyberwar when all signs predicted its onset, and the bare indictment's effectiveness as a deterrent measure stemmed from its grounding in domestic criminal law. Not only was this domestic grounding responsible for the bare indictment's ability to humiliate Iran and hence deter without angering, but it also established the bare indictment's legitimacy under international law, making its issuance as a deterrent measure incontestable from a practical legal standpoint. The insights from this case study suggest that bare indictments may be leveraged as an effective measure for addressing cyberattacks that may be construed as acts of cyberwarfare – and perhaps, under the principles of *ius ad bellum*, as a requirement to fulfill a state's responsibility to avert cyberwar.

The examination of the U.S. Financial Industry DDoS case study directly informs the analysis of the ongoing hybrid war between Russia and Ukraine; the demonstrable success of bare indictments as a de-escalatory measure generates appurtenant suggestions for using domestic criminal charges not only to speed a resolution to this conflict, but also to set general deterrent norms against future hybrid wars that may otherwise arise.

8.2.0. Bare Indictments Affirm The Issuer's State Sovereignty, Potentially Denying the Motives of Russian "Hybrid Warfare" Cyberattacks

In Section 5.4., I suggested that Russia could have more effectively garnered the favor of the U.S. if the Russian FSB had participated in a cooperative effort with the American FBI to jointly investigate the Colonial Pipeline cyberattack. The prospect of U.S.-Russia collaboration on cybersecurity matters, along with any likelihood that the U.S.'s favor would sway toward Russia, was soon eliminated by Russia's invasion of Ukraine on February 24, 2022. This military conflict, still ongoing as of the time of this writing, has been accompanied by cyberattacks that have been designed to disable Ukrainian computer systems; considering that these cyberattacks have been technically attributed to Russian state-sponsored actors such as Sandworm, they provide an example of "hybrid warfare" tactics used by the Russian state. Given that both the cyber means and the criminal nature of these cyberattacks resonate with the literature of hybrid warfare, I extrapolate from the theory on bare indictments and draw from insights of previous case studies to suggest how bare indictments may be leveraged to set a norm against the Russian state's conduct and deter like conflicts from being instigated in the future. Conducting an analysis of the motives behind these cyberattacks supports an argument that the cyberattacks are part of the Russian state's overarching dominance-seeking motivations for waging hybrid war against Ukraine. If these are dominance-seeking cyberattacks, then bare indictment should be able to deter further cyberattacks by denying their expected benefit of status. Even more so, the role of criminal charges in invoking CDT's constitutive function of the state directly counteracts the Russian state's arguable objective to suppress and eradicate Ukraine's state sovereignty; thus, the theory predicts that the issuance of bare indictments

not only will achieve a highly specialized specific deterrent effect by targeting the Russian state's prestige-seeking goal of "de-Ukrainization," but also will achieve general deterrence against the future initiation of hybrid warfare that seeks to suppress a target nation's sovereignty. As was suggested in Section 7.1., bare indictments' ability to serve as a bluff is not a detriment, but rather, is crucial in achieving optimal deterrent effects.

In this section, I first present the definition of hybrid warfare and show why the concept suggests a place for CDT to harmonize with SDT so as to formulate optimal deterrent measures against a threat that combines criminal acts with military conflict. Then, I briefly review scholarly analyses further showing why Russia's February 2022 military invasion of Ukraine is characterizable as hybrid warfare. Drawing from the theoretical framework on bare indictments, I next determine the motives for Russia's hybrid warfare cyberattacks. I look to the public statements of Russian President Vladimir Putin to determine that the overarching motivations of the cyberattacks are primarily dominance-seeking, and that they have the particular objective of suppressing Ukraine's statehood. Because domestic criminal charges carry out CDT's constitutive state function of administering the criminal law to prevent harm from coming to a state's inhabitants, the issuance of bare indictments against these cyberattacks is predicted to deter Russia not only by frustrating its dominance-seeking motivations, but also by counteracting its objective of suppressing Ukrainian state sovereignty.

The central policy recommendation in this ongoing conflict is that the Ukrainian state issue domestic criminal charges against Russian state-sponsored cyberattackers. I address a potential counterargument on the corruption of Ukraine's judiciary to show why

bare indictments' function as a bluff enables optimal deterrence: since bare indictments will most likely remain "bare," the deterrent effect can be achieved without having to reach the trial stage. I also consider this policy suggestion's interaction with the SDT concept of "extended deterrence," or executing deterrent measures on behalf of one's allies. I next address the counterargument that nation-state cyber adversaries may issue their own domestic criminal charges in response. Finally, I briefly recount reflections on the use of domestic criminal charges to strengthen state sovereignty and set general deterrent norms.

8.2.1. The First Hybrid War

According to John G.L.J. Jacobs and Martijn W.M. Kitzen (2021), the "first definition of hybrid warfare in academic published work" came in a 2007 paper by military scholar Frank G. Hoffman. Hoffman's definition of "hybrid warfare" concerns the melding of "conventional" military forces with non-conventional means of attack, such as criminality: "Hybrid Wars incorporate a range of different modes of warfare, including *conventional capabilities*, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and *criminal disorder* [emphasis added]" (2007, 14). Hoffman theorized that criminality would serve an instrumental role in weakening and destabilizing the target of hybrid warfare, rendering it more vulnerable to an attack by conventional military forces: "Criminal activity is used… to facilitate the disorder and disruption of the target nation" (2007, 30). Hoffman conceptualized hybrid warfare as blending conventional with non-conventional not only with respect to the type of attack, but also the "means" of attack (2007, 28). For example, a hybrid war could combine conventional

military warfare with cyber warfare, especially "cyber-warfare directed against financial targets" (Hoffman 2007, 28).

Due to its accompaniment by cyberattacks, the military invasion of Ukraine by Russia has been conceptualized as a hybrid war. True to Hoffman's predictions, it appears that Russian state-sponsored actors deployed cyberattacks designed to damage Ukrainian state and civilian computer systems to 'weaken and destabilize' the Ukrainian target. In a February 25, 2022 article entitled "The hybrid war that began before Russia invaded Ukraine," reporter Frank Hofmann[24] wrote that disabling cyberattacks seemed to have been mounted in preparation for Russia's military invasion: "On February 23, the eve of the first Russian missile strikes on Ukraine, international cyber-security researchers at security company ESET had already registered cyber-attacks on numerous computers in Ukraine. The company discovered what is known as a 'wiper' attack... It has no other purpose than to make the computer inoperable" (Hofmann 2022). Similarly, in the weeks before Russia's military invasion, DDoS cyberattacks were mounted against Ukrainian state targets such as its "defense ministry" (Hofmann 2022). Moreover, these disabling cyberattacks were mounted against 'financial targets'; Hofmann reported that DDoS cyberattacks had rendered inaccessible to users "the online banking [systems]" of "two large Ukrainian banks" (2022).

While cyberwarfare had arguably been waged before, the blending of conventional military warfare and cyberwarfare in this configuration of hybrid warfare appeared to be unprecedented. Two arguable examples of cyberwarfare – both of which are mentioned in

[24] The similarity in the names of military affairs scholar Frank G. Hoffman and reporter Frank Hofmann appears to be coincidental.

this project – include the 2007 DDoS cyberattacks against Estonia, which were technically attributed to Russian state-sponsored actors; and the 2011-2013 U.S. Financial Industry DDoS attacks, which a U.S. bare indictment alleged had been perpetrated by Iranian state-sponsored cyberattackers. While cyberwarfare – without accompaniment from conventional military attacks – had been waged in years before, the hybrid warfare initiated in February 2022 was apparently the first conflict in which a military invasion was facilitated by cyberattacks. During a press conference given in early March 2022, Ukrainian state cybersecurity official Viktor Zhora described the cyberattack-enabled military conflict between Russia and Ukraine as a "hybrid war" that was "happening for the first time in history" (Tidy 2022).

8.2.2. Analysis of Russia's Dominance-Seeking Motives in Suppressing Ukrainian Statehood

Notwithstanding these cyberattacks' deployment in hybrid warfare, the behavioral analysis method of determining motive from the circumstances of the offense and the identity of the target may still be applied to yield an arguable result that the cyberattacks were dominance-seeking. Looking first to the circumstances of the cyberattack, it is clear from the type of cyberattacks – DDoS and "wiper malware," rather than unauthorized access leading to data theft – that the aim of these targets was to disable the Ukrainian civilian and state targets rather than to obtain something of economic value. Thus, the cyberattacks were probably not profit-seeking. As mentioned above, an analogy can be drawn to the 2007 DDoS cyberattacks against Estonia and the 2011-2013 U.S. Financial Industry DDoS attacks, both of which were arguable instances of cyberwarfare that this

project argues were primarily motivated by dominance-seeking. Just as wars – including these arguable cyberwars – have been initiated over status, the cyberwarfare component of Russia's hybrid warfare seems to be primarily status-seeking via dominance-seeking.

The primacy of the dominance-seeking motive becomes even clearer when one expands the scope of analysis to the overarching objective of the *warfare* that these cyberattacks facilitate. Statements from Russian state leadership, as well as Russian military forces' targeting of Ukrainian cultural symbols, support a contention that not only the cyberwarfare component but also the hybrid war as a whole is primarily motivated by dominance-seeking. Suzanne Nossel, writing in *Foreign Policy*, points to Putin's public statements as evidence that the Russian state's objectives in the invasion center on suppressing Ukraine's state sovereignty: "In a televised address launching the war, Putin denied that Ukraine had ever enjoyed 'real statehood' and claimed the country as part of Russia's 'own history, culture, spiritual space'" (Nossel 2022). Nossel points to reports that besides the many "cultural sites" including "museums, historic buildings, libraries, and religious institutions" that have been destroyed in Russia's invasion, Russian military forces "torched" Ukrainian cultural archives in a destructive action that has no apparent military purpose (Nossel 2022). Likewise, a report from *NBC News* states that allegations have surfaced that the Russian state's destruction of Ukrainian cultural sites is largely deliberate: "Since Russia launched its invasion of Ukraine on Feb. 24, Ukrainian officials have accused Moscow of intentionally attacking hundreds of cultural sites... Ukrainians say the attacks are part of Russian President Vladimir Putin's effort to erase Ukrainian identity" (Egan 2022).

While the counterargument might be made that Russian military forces' reported destruction of Ukrainian cultural sites is collateral damage of military activity rather than an attempt to suppress Ukrainian culture, evidence has emerged that contradicts such a counterargument. The *NBC News* report covers the example of the long-distance bombing of a museum in a Ukrainian village that had "no legitimate military targets": "military analysts who, at the request of NBC News, reviewed photos of the damaged museum... said that precision-guided munition – which is used to hit a very specific target – was likely used by Russia to intentionally destroy the museum" (Egan 2022). Providing further supporting evidence, Jeffrey Mankoff's April 22, 2022 report published through the Center for Strategic and International Studies argues that contextualizing Putin's objective as a forcible attempt to subsume Ukrainian state "identity" within Russia "helps explain Russia's military strategy" (Mankoff 2022, 2). Mankoff's argument resonates with the second part of prestige-seeking, since Mankoff argues that Russian state leadership miscalculated the views of other members of the global society (2022, 2). According to Mankoff's analysis, Russia mistakenly believed that Ukrainians "would accept some form of reintegration into a Russian sphere of influence" (Mankoff 2022, 2). Russia's miscalculation further evidences the dominance-seeking motive of this hybrid warfare; in suppressing Ukrainian statehood, Russia's belief that other nation-states would accept its bid for high rank in the social hierarchy of the international community implies Russia's pursuit of not only a high status, but also of being *viewed* as high in status. As Nossel argues, "Russian President Vladimir Putin has targeted his campaign against Ukraine not just to seize territory or subdue resistance but to subsume Ukraine culturally, linguistically, and territorially into Russia, denying its existence as a sovereign, independent nation" (2022). Hence, the cyberattacks

can be seen as a component of Russia's overarching dominance-seeking attempt to increase its rank in the social hierarchy of the international community, suppressing Ukraine's statehood via destroying symbols of Ukrainian culture.

8.2.3. Ukraine Should Issue and Publicize Domestic Criminal Charges to Deter Hybrid Warfare

With the cyberattacks being primarily motivated by dominance-seeking, the theory on bare indictments would predict that if Ukraine – the target of the cyberattacks – were to issue and publicize domestic criminal charges against the apparently Russian state-sponsored cyberattackers, the informal sanctions triggered by being labeled a "criminal outcast" would have both specific and general deterrent effects by directly denying the Russian state its expected benefit of status. Furthermore, if Russia's expected benefit from waging hybrid warfare against Ukraine is conceptualized not just as falling within the category of dominance-seeking motives, but also as the expected benefit of suppressing Ukrainian sovereignty and statehood, then the deployment of Ukraine's domestic criminal law may be predicted not only to deter the cyberattacks, but also to have deterrent effects against the hybrid warfare as a whole.

As discussed in Chapter 2, the classical CDT writers Beccaria and Bentham saw the essential constitutive function of statehood – the defining action of a state – as imposing punishments pursuant to the criminal law, since criminal law stems from every state's duty to protect its members from harm-causing actions that have been deemed crimes. Beccaria's and Bentham's conception of criminal law as stemming from this state's duty to protect coincides with the conception of criminal law laid out in Chapter 1, Article 2,

Section 1 of the Criminal Procedure Code of Ukraine, which begins, "The objectives of criminal procedure are the protection of individuals, society, and the state from criminal offence…" If Russia's expected benefit in this hybrid war is to suppress Ukrainian statehood, then Ukraine's issuing domestic criminal charges to impose the punishment of informal sanctions in response to Russia's actions would be predicted to directly frustrate Russia's expected benefit, since imposition of punishment pursuant to the criminal law is a defining characteristic of statehood that resonates with codified law in the Ukrainian context.

Drawing insights from prior case studies helps inform the policy recommendation. Recall that, as discussed in Section 7.6., the United Kingdom is a jurisdiction wherein the standard procedure is for criminal charges to be issued *upon* apprehension, whereas in U.S. federal criminal procedure it is standard procedure for criminal charges to *precede* and provide grounds for apprehension. Therefore, it was suggested that, in the UK, the equivalent procedural action to impose the punishment of informal sanctions and publicize such imposition was to authorize the police to issue criminal charges and publicly announce that the police had been so authorized. Based on Article 42, Section 1 of the Ukraine Code of Criminal Procedure, it appears that the equivalent procedural action to issuing domestic criminal charges that would trigger the package of informal sanctions is issuing a "notice of suspicion." According to Article 42, Section 1, it seems that the standard procedure is for the notice of suspicion to be delivered upon apprehension, or at least to be delivered to the accused individual, implying that the individual must have already been located. However – unlike the UK's criminal procedure – Article 42, Section 1 implies that Ukraine's domestic criminal charges can be issued before the accused individual is located,

as Article 42, Section 1 contemplates situations in which "a notice of suspicion has been compiled but it has not been delivered because of failure to establish the whereabouts of the person." Thus, the equivalent policy recommendation to the U.S.'s issuance and public announcement of a bare indictment would be Ukraine's issuance and public announcement of a notice of suspicion against suspected Russian state-sponsored cyberattackers. Where the law criminalizing cyberattacks would be 18 U.S.C. § 1030 in the U.S., Article 361 of the Criminal Code of Ukraine – "Willful interference with the operation of computers, computer systems and networks" – would probably be the most appropriate law under which a notice of suspicion could be issued for cyberattacking activity.

8.2.4. Optimally Deterring Hybrid Warfare without Having to Follow Through on Bluffs

Looking to bare indictments' ability to serve as a bluff shows that Ukraine's issuing "bare" domestic criminal charges against suspected Russian cyberattackers would further enable the optimization of this deterrent measure. It first bears mentioning that criminal charges issued by Ukraine against Russian nationals could be considered "bare"; Ukraine and Russia do not appear to have any bilateral extradition treaty between them, and although the two nations are each parties to two multilateral extradition treaties, the terms of these two multilateral extradition treaties are subject to many exceptions that could easily and straightforwardly be cited such that Russia would almost never have a legal obligation to extradite a Russian national to Ukraine (Bilych et al. 2014, 8).

A possible concern with Ukraine's issuing domestic criminal charges is that, as of late 2021, it is apparently common knowledge in the international community that

Ukraine's judiciary is "notoriously corrupt" (Hardie 2021); in September 2021, European and American diplomats officially demanded that Ukraine implement judicial reforms (RFE/RL 2021). If Ukrainian judges – responsible for overseeing a domestic criminal trial – cannot be trusted to perform their duties properly, then would domestic criminal charges in Ukraine be too subject to accusations of corruption, undermining the deterrent effect? A rebuttal to such a counterargument would be that it is precisely because "bare" domestic criminal charges are unlikely to result in trial, much less conviction, that they are an optimal deterrent measure. In accordance with the discussion in the PLA Unit 61398 case, domestic criminal charges should not be used as empty bluffing, but domestic criminal charges *can* operate under the assumption that it is highly unlikely that the charged individuals will ever "call the bluff" by 'voluntarily' coming to face trial. Since it is unlikely that individuals against whom bare criminal charges have been issued will face trial, the concern about corruption of the judiciary would occur at a procedural stage – trial – that will probably not be reached. As has been argued throughout this project, it is the stage at which the bare criminal charges are issued and publicly announced that triggers the package of informal sanctions, including the attack on face that can directly frustrate status-seeking objectives.

8.2.5. Denying Russian National Status; Legal Jurisdiction and Extended Deterrence

From the case of the FSB's arrest of the Colonial Pipeline actors, it can be learned that Russia – while arguably less sensitive to attacks on face than is China – seemingly did change its behavior in response to bare indictments' continued attacks on Russian national

face. Notwithstanding that the bare indictments were issued against profit-seeking non-state cyberattackers, *respondeat superior* and the principle of responsibility imputation in attribution theory meant that Russia was apparently embarrassed by bare indictments' making it common knowledge that Russia had failed to control the non-state cyberattacking activity. If Russia could see the indictments of profit-seeking non-state actors as a threat to national status, then issuing bare criminal charges against *status-seeking state-sponsored* Russian cyberattackers should have an even stronger effect on frustrating the Russian state's status-seeking objectives. To make it more likely that the necessary condition for *respondeat superior* to apply will be fulfilled, any criminal charges filed against suspected Russian hybrid warfare cyberattackers should expressly establish an allegation of Russian state sponsorship to support the perception that Russia could and should have done something to prevent the cyberattacks.

When issuing charges under domestic criminal law against state-sponsored actors, the issue of extended deterrence in SDT is a problem of credibility and legitimacy. Michael J. Mazarr's piece on "Understanding Deterrence" of nation-states in world politics (2021, 15) reviews the issue of "extended deterrence": "discouraging attacks on third parties, such as allies or partners" (Mazarr 2021, 16). Mazarr links the issue of extended deterrence back to the credibility problem in SDT, since "An aggressor can almost always be certain a state will fight to defend itself, but it may doubt that a defender will fulfil a pledge to defend a third party" (2021, 16).

In the context of using domestic criminal law as a deterrent measure against international cyberattacks, I would point out two reasons why allies' actions in furtherance

of extended deterrence would be limited. One – given that classical CDT writers theorized that taking action under domestic criminal law is a constitutive function of statehood – having another nation-state issue domestic criminal charges for cyberattacks that did not obviously directly affect its own affairs or geographic territory would not as readily communicate the affirmance of sovereignty that I theorize could serve as a deterrent measure when such sovereignty is under attack. If, for instance, the UK were to take action pursuant to the domestic criminal law in defense of Ukraine's interests, classical CDT would view that action as an affirmation of the UK's statehood more than of Ukraine's. Two, allies' responses under their domestic criminal laws would probably not satisfy the requirement of domestic territorial jurisdiction in criminal law; since the legitimacy of such responses would be disputable by other members of the international community, the extended deterrent effect would likely be weakened. Having another nation-state take action pursuant to domestic criminal law for cyberattacks that did not obviously directly affect its own affairs or geographic territory might not satisfy legal requirements for extraterritorial applicability of domestic criminal law (see Doyle 2016), and therefore would likely require such action's being grounded in the legal principle of universal jurisdiction (Randall 1987). Although establishing universal jurisdiction is not an insurmountable hurdle, the legitimacy of universal jurisdiction is subject to more question. Universal jurisdiction is a principle pertaining to international law, and international law as a whole has been susceptible to questions of legal legitimacy (Wolfrum 2021; Thomas 2014), especially as it may be argued that international law compromises state sovereignty (see Yannis 2002). By contrast, situating an action firmly within domestic criminal law invokes the state's duty to protect its members and hence *affirms* state sovereignty. As this

project discussed in the U.S. Financial Industry DDoS Attacks case study of cyber warfare, Matthew J. Aiesi and Amanda L. Minikus have argued that establishing legal legitimacy in actions taken to respond to warfare is not just an ethical but also a practical matter, as establishing legitimacy can help rally international support and lower the likelihood that other members of the international community will protest such action (2020).

I suggest, therefore, that justifying deterrent measures within the sphere of domestic criminal law can be a 'fast-track' to establishing legal legitimacy. This is irrespective of whether international law would *also* be applicable, as jurisdiction under domestic versus international law is not necessarily an either-or question. Logically, a given offense may be both a "war crime," meaning the offense is a violation of the international laws of war (United Nations, "War Crimes," n.d.); and a violation of domestic criminal law. However, I would point out that due to the circumscribing principle of territorial jurisdiction in domestic criminal law (Berge 1931; Perkins 1970; Randall 1987, 785) and the delimiting "principle of non-intervention" in international law (Green 2015b, 108), justifying state action pursuant to domestic criminal law may tend to be more straightforward and less controversial than arguing that some offense qualifies as a war crime under international law. This may be especially true where cyberattacks are concerned, given the relative novelty of cyber warfare. Commentators have argued that the alleged Russian cyberattacks that preceded the February 2022 invasion of Ukraine *should* be considered war crimes (Burkhalter 2022; see also Greenberg 2022). While this contention may be debatable, there would be almost no question that the alleged Russian cyberattacks are violations of Article 361 of the Criminal Code of Ukraine.

8.2.6. Optimizing Global Norm-Building and Extended Deterrence [RUSS-05] [RUSS-06]

Although criminal law's being a constitutive function of statehood and domestic criminal jurisdiction's being territorially constrained mean that it would not be an optimal deterrent measure for Ukraine's allies to issue domestic criminal charges *on behalf of* the Ukrainian state, this discussion suggests that there are multiple ways that Ukraine's allies can contribute to norm-building extended deterrence. One of these ways, following a putative lesson learned from the APT40 case study, is by allies' issuing their own domestic criminal charges in response to Russian state-sponsored cyberattacks committed against computer systems within their respective territorial jurisdictions.

The United States has already done so, as the most recent set of bare indictments issued under 18 U.S.C. § 1030 and publicized by the DOJ was unsealed and publicly announced by the DOJ on March 24, 2022. Both of these bare indictments portrayed the defendants as Russian state-sponsored cyberattackers. The first indictment, which had been filed on June 29, 2021, alleged that the defendant had committed cyberattacks against U.S. energy facilities while he was an employee of the Russian Ministry of Defense (*Gladkikh* indictment, 2-3); accusing this suspected cyberattacker of having been in the employ of a Russian government agency established the *respondeat superior* condition for responsibility imputation to the Russian state. The second bare indictment that the DOJ unsealed and announced on March 24, 2022 had been filed on August 26, 2021. It alleged that three officers of the FSB had executed cyberattacks against "hundreds of U.S. and international energy sector companies" (*Akulov* indictment, 5); these cyberattacks would

have "enabled the Russian government to disrupt and damage" the computers controlling "power generation" (*Akulov* indictment, 3). Like the indictment against the alleged Lazarus North Korean state-sponsored cyberattackers, this indictment situated the cyberattacks under domestic criminal law yet portrayed them as an international concern: "hundreds of foreign victims… were based in over 135 countries" (*Akulov* indictment, 7). Especially as reports have surfaced that Russian nationals have been mounting cyberattacks against computer systems under the domestic territorial jurisdiction of the U.S. and other nation-states besides Ukraine, a policy recommendation is for the U.S. and other nation-states to proceed with issuing domestic criminal charges in response to cyberattacks technically attributed to Russian nationals.

From the Seleznev case, it may be learned that the law enforcement authorities of Ukraine's allies – by assisting Ukraine in apprehending individuals who have been criminally charged by Ukraine – can also bolster the deterrent force of any "bare" domestic criminal charges that Ukraine issues. Nation-state allies who wish to contribute to deterring Russian state-sponsored cyberattacks could help enforce not only Ukraine's, but also *each other*'s, domestic criminal charges issued against suspected Russian state-sponsored cyberattackers; allies may strengthen the deterrent effect of "bare" criminal charges by cooperating in apprehending and extraditing these individuals to the country that has issued the charges against the individuals, irrespective of whether a legal obligation under treaty requires the ally to do so.

While the domestic criminal charges – to have optimal deterrent effect – must ultimately be issued by Ukraine rather than by one of Ukraine's nation-state allies, nation-

state allies as well as non-governmental organizations can assist by lending investigatory support to help compile the factual evidence necessary to compile criminal charges under Article 361 of the Criminal Code of Ukraine. International allies, nation-state and non-governmental alike, have been mobilizing to assist Ukraine with its war crimes prosecutions; as these war crimes are matters of international law, I would suggest that such aid may consider assisting Ukrainian prosecutors in investigating cyberattacks and pursuing domestic prosecutions of such cyberattacks as well.

To contribute to extended deterrence, private cybersecurity firms can also play an important role in providing technical attribution results. For example, in the PLA Unit 61398 case, the 18 U.S.C. § 1030 bare indictment drew from the technical attribution results in the 2013 Mandiant report, including Mandiant's technical attribution of an individual whom the bare indictment eventually named as lead defendant (Goldsmith 2014, Mandiant 2013). As Goodman (2010) and Healey (2011) each theorized, technical attribution results must be mobilized in order to achieve any political effect. Another way to look at this situation is that domestic criminal charges need technical attribution results so as not to be empty bluffs; thus, private cybersecurity firms can use their resources and the expertise of their cybersecurity researchers to shoulder the task of arriving at the technical attribution results that may then be relied upon for a nation-state to issue domestic criminal charges against the perpetrators of these cyberattacks.

///

///

8.2.7. What If Russia Issues Its Own Bare Indictments?

To raise a final objection, a counterargument that this project has heretofore not discussed might be especially pertinent to address here. Some scholars, such as Dave Aitel, have argued that a reason militating in disfavor of the issuance of U.S. bare indictments against the intelligence agents of nation-state cyber adversaries is that nation-state cyber adversaries might, reciprocally, issue their own domestic criminal charges against U.S. nationals and U.S. intelligence agents (Aitel 2016), especially since it is speculated that the U.S. government engages in international cyberattacking activity as well (Zegart 2020). What if the U.S.'s cyber adversaries start issuing their own domestic criminal charges against alleged U.S. state-sponsored cyberattackers?

Similarly, following the Russian state's February 2022 initiation of hybrid warfare against Ukraine, the Ukrainian state formed an "IT Army" made up of Ukrainian and international volunteers who would carry out cyberattacks on behalf of Ukraine (Shore 2022). Writing in *Foreign Policy*, Jennifer Shore described the unprecedented call to action from Ukrainian state leadership amidst the hybrid warfare between Russia and Ukraine: "on Feb. 26, Ukrainian Vice Prime Minister Mykhailo Fedorov took a step no other government official in the world likely ever has: He publicly called on volunteer hackers to take down another country's websites. And he had a list of 31 Russian government, bank, and corporation websites ready to go. Within days, Ukraine had amassed an "IT army" of more than 400,000 volunteers" (Shore 2022). Shore describes that the IT Army has claimed responsibility for mounting successful DDoS cyberattacks against numerous "Russian civilian and government websites" (Shore 2022). In an interview with *Wired* that was published on June 02, 2022, Ukrainian President Volodymyr Zelenskiy expressly

praised the efforts of the IT Army, describing it as "Our [Ukraine's] IT Army" (Cain 2022). Because Ukrainian governmental officials – in their official capacity, no less – expressly encourage and condone the cyberattacks carried out by the IT Army, the principle of responsibility imputation and *respondeat superior* would clearly apply for responsibility for these cyberattacks to be imputed to the Ukrainian state. What if the Russian state issues and publicizes its own domestic criminal charges against these Ukrainian state-sponsored cyberattackers and the cyberattackers of Ukraine's allies?

My answer – which is also apposite to the U.S. scenario – is that, all things considered, this should not be a matter of great concern for Ukraine and its allies; the issuance of bare indictments by the Russian state will not trigger any informal sanctions that would deter the IT Army. In the U.S. scenario, it is speculated that the U.S. government's cyberattacking activity largely has an intelligence-gathering purpose. I argued, in my analyses of Chinese and Iranian trends toward profit-seeking, that it would be imprecise to argue that bare indictments cannot deter espionage operations; an example of such an argument is found in Amy Zegart's piece "Everybody Spies In Cyberspace" (2020). The case studies examined in Section 4.5. and Section 4.6. show that it would be more precise to argue that bare indictments do not tend to deter *profit-seeking* espionage operations, since informal sanctions are unlikely to deny or outweigh the profit-seeking motive. Because U.S. government cyberattacking activity is speculated to be conducted mainly for intelligence-gathering purposes, alleged U.S. government cyberattacking activity would best be characterized as primarily profit-seeking given the valuable nature of data. This is in contrast to much of the Chinese cyberattacking activity described in Chapter 4; although many of those cyberattacks were fairly characterizable as espionage, the

espionage operations were often primarily motivated by prestige-seeking rather than profit-seeking, and data analysis of the trend supported an argument that informal sanctions triggered by bare indictment achieved a general deterrent effect against prestige-seeking cyberattacks but not against profit-seeking cyberattacks. Correspondingly, if any other member of the international community issues bare domestic criminal charges in response to the U.S. government's suspected cyberattacking activity, the informal sanctions will not deter the U.S. government's suspected profit-seeking cyberattacking activity. Even cumulative attacks on the U.S.'s prestige should have little effect; unlike the Russian state's embarrassment over its failure to curtail the cyberattacking activity of Russian non-state profit-seeking cyberattackers, the U.S. would likely stand behind the U.S. government cyberattacking activity under its control.

While the IT Army's cyberattacking activity – like the cyberattacking activity of some indicted Russian state actors – is not easily categorizable in the framework of status-seeking, thrill-seeking, and profit-seeking, the same conceptual consideration can be applied to yield the predicted results. In Chapter 5, I discussed that if the expected benefit were quantified as the objective of disinformation, informal sanctions would neither deny nor outweigh this objective. Analogously, if the objective of the IT Army's cyberattacks is quantified as 'defending Ukrainian computer systems from Russian cyberattacks,' then informal sanctions will neither deny nor outweigh this objective. It seems unlikely that the other members of the international community will give much credence to Russia's attacks on Ukrainian prestige, but *even if the international community did*, then the informal sanction of an attack on face would not directly frustrate the expected benefit of preserving Ukrainian computer systems.

The practical consequences in the package of informal sanctions may be worth considering, since "bare" indictments do not necessarily remain "bare," but it should usually be relatively straightforward and not particularly difficult to ensure that the risk of apprehension never becomes an actual apprehension. Individuals need only refrain from traveling to Russia and refrain from traveling to any jurisdictions that are likely to cooperate with Russian law enforcement. Some examples of such jurisdictions would arguably include Tajikistan and Uzbekistan, since Russia has recently cooperated with extradition requests from those countries (Armitage 2013) and may expect reciprocal cooperation from them in the future. It seems that most national jurisdictions do not have a bilateral extradition treaty with Russia. However, these jurisdictions may have some limited legal obligations under a MLAT or MLAT-like instrument to assist or share information with Russian law enforcement, may have some limited legal obligations under a CMAA or CMAA-like instrument to assist or share information with Russian law enforcement, and may also have discretionary power to grant Russian law enforcement's requests for assistance or information-sharing. The U.S., for instance, finds itself in this situation.

To ease defensive cyberattackers' fears of being apprehended and extradited to Russia, I suggest that such jurisdictions publicly issue a policy directive to make common knowledge what might previously have been arguably obvious, but not common knowledge: in the absence of legal obligation, the jurisdiction will decline to cooperate with any extradition requests from the Russian state and will decline to cooperate with information-sharing requests from Russian governmental law enforcement. A publicized policy directive thusly worded would not make such jurisdictions run afoul of any of their

existing legal obligations toward Russia – although whether such jurisdictions *should* openly run afoul of their existing legal obligations toward Russia is a question I leave for consideration by other scholars. Given the limited scope of legal obligations under MLAT-like or CMAA-like treaties, it should be relatively straightforward for these jurisdictions to argue in most cases of Russian requests for assistance or information-sharing that a legal obligation does *not* apply.

Considering that state-sponsored cyberattackers and states may take steps to ensure that "bare" criminal charges from Russia remain bare, the state-sponsored cyberattackers and states might be well advised to follow Aiesi and Minikus' suggestion of establishing legitimacy before other members of the international community. I suggest that these states and state-sponsored cyberattackers can, in many cases, preemptively establish the legitimacy of cyberattacks against Russia by positioning those cyberattacks as defensive, as did Zelenskiy in the June 02, 2022 *Wired* interview (Cain 2022; see also Burgess, February 27, 2022). In the international laws of war, self-defense is an exception that legitimates a state's use of force (International Committee of the Red Cross 2022). Similarly, in domestic criminal law, self-defense is a justification that makes allegedly "criminal" actions no longer criminal; legal scholar Michael M. O'Hear calls the self-defense justification "a well-established, noncontroversial aspect of criminal law" (O'Hear 2008). Further analysis of whether self-defense applies as an exception and / or justification for the IT Army's cyberattacking activity is another question I leave for consideration by other scholars, in light of relevant factual evidence that may emerge.

In the hypothetical situation of cyber adversaries such as Russia imposing domestic criminal charges against the U.S., Ukraine, and Ukraine's allies, the informal sanctions triggered by bare indictment would be predicted to have no deterrent effect. The hypothetical results of Russia's imposing domestic criminal charges against U.S. and Ukrainian cyberattackers would be comparable to the results of Russia's March 15, 2022 imposition of economic sanctions against U.S. federal government officials including U.S. President Joe Biden. Like the practical consequences triggered by these economic sanctions, the practical consequences triggered by a Russian bare indictment may be easily avoided and may not even require a change in behavior. As *CNN* reported, U.S. White House press secretary Jen Psaki publicly proclaimed at a press briefing that the economic sanctions issued by Russia would have no deterrent effect toward any U.S. operations: "It won't surprise any of you that none of us are planning tourist trips to Russia, none of us have bank accounts that we won't be able to access, so we will forge ahead" (Vasquez 2022). Besides individuals being mindful not to travel to Russia – nor to any jurisdictions that are likely to grant extradition, assistance, or information-sharing requests from the Russian state – Ukrainian state-sponsored cyberattackers, the Ukrainian state, and allies of Ukraine should pay any Russian domestic criminal charges little heed.

8.2.8. General Deterrent Norms against Status-Seeking Hybrid Warfare

The preceding case studies have culminated in informing the policy recommendations on how both the U.S. and other nation-states may leverage bare indictments to achieve a deterrent effect against suspected Russian state-sponsored

cyberattackers amidst the Russian state's hybrid war against Ukraine. By affirming state sovereignty, charges under domestic criminal law may be effective against deterring international cyberattacks even when – or perhaps, because hybrid warfare can meld the criminal with the military, *especially* when – cyberattacks are executed as part of hybrid warfare. Moreover, by making it common knowledge that the status-seeking objectives of the Russian state have been frustrated, "bare" domestic criminal charges may go so far as to achieve some general deterrent effect against the initiation of such status-driven conflicts in the future.

CHAPTER 9

CONCLUSION: A GLOBAL FUTURE FOR CRIMINAL DETERRENCE THEORY

9.0. Transcending Boundaries in Combating Cyberattacks

In his remarks on the U.S. Financial Industry DDoS Attacks, Manhattan U.S. Attorney warned that the threats of the global future transcended national borders and could be mounted from afar: "We now live in a world where devastating attacks on our financial system, our infrastructure, and our way of life can be launched from anywhere in the world, with a click of a mouse" (USAO SDNY, March 24, 2016). It is perhaps fitting, then, that bare indictments – measures of domestic criminal law – can likewise be administered irrespective of geographical distance in order to effectively counter these cyberattacks.

Cyberattacks waged by foreign nationals blur not only the boundaries between nations, but also the boundary between the domestic and the international. It is in light of this permeability between matters of domestic and international concern that, despite seemingly being unable to accomplish any deterrent effects, domestic criminal charges can deter international cyberattacks. Even when the accused cyberattacker is a state actor, the salience of a status-seeking or thrill-seeking motive can render the accused cyberattacker vulnerable to informal sanctions that deny the expected benefit of status and outweigh the expected benefit of emotional thrill. When bare indictments – which can be likened to impositions of punishment in classical CDT – are made public, then the informal sanctions they trigger can serve both to specifically deter the individuals against whom they are issued, and to generally deter other individuals who might otherwise carry out cyberattacks. Since accused individuals and other potential offenders seek to avoid

apprehension, a bare indictment need not ultimately result in apprehension to achieve deterrence; it is at the stage at which a bare indictment becomes common knowledge that it achieves optimal deterrent effects.

The deterrent force of bare indictments is not merely theorized, but rather, is supported by empirical evidence. Analysis of the case studies in this project has shown, for example, that the start of the dramatic decline in Chinese cyberattacking activity coincided with the DOJ's announcement of the bare indictment against five members of PLA Unit 61398. Similarly, the SamSam Ransomware cyberattackers were still actively engaging in cyberattacking activity days before the publicization of a bare indictment accusing two individuals of perpetrating this cyberattacking activity, yet SamSam Ransomware schemes came to an abrupt stop after the indictment was made common knowledge. In such case studies, the before-and-after study design yielded evidence showing that it was likely that deterrent effects were achieved by bare indictment.

With the theory having been supported by empirical evidence, the theory on bare indictments provides a lens through which to clarify the actions of nation-states such as Russia. The theory on bare indictments speaks to the debate over whether Russia's cooperation with the U.S. in apprehending a Russian non-state cyberattacker was an attempt to curry favor or – as I have argued – a bid to avoid embarrassment.

Part of the reason why bare indictments carry deterrent force is that the data shows they have not remained as "bare" as might previously have been thought; the Su Bin and Arrow Tech cases, as well as many of the numerous cases on profit-seeking Russian non-state actors, involved arrests and convictions pursuant to bare indictment. On the other

hand, when bare indictments achieve deterrent effects without having to result in apprehensions and prosecutions, they can be seen as a cost-effective and hence optimal deterrent measure – a bluff upon which the issuer never needs to follow through.

This project shows that understanding and leveraging the theory on bare indictments can yield numerous insights for policy practitioners. For instance, economic sanctions should *not* be blindly imposed in conjunction with § 1030 bare indictments, since the imposition of economic sanctions can interfere with bare indictments' deterrent effect. In contemporary context, arguably even more compelling is that the insights from case studies speak to conflict de-escalation amidst an ongoing hybrid war; the theory on bare indictments may be extrapolated to inform next actions for the international community to domestically respond to Russia's February 2022 invasion of Ukraine such that making common knowledge the denial of Russia's status-seeking objectives may also achieve a general deterrent effect against the initiation of future conflicts.

As a direction for future research, it would be interesting to examine to what extent the permeability between domestic and international may extend down to the provincial level. To set norms internationally, perhaps domestic criminal charges could be issued under provincial law in addition to, or instead of, under national law. According to the National Conference of State Legislatures, as of May 04, 2022 all fifty states in the U.S. have provincial laws criminalizing cyberattacks *qua* unauthorized access; moreover, many have provincial laws criminalizing cyberattacks as causing damage to computer systems (National Conference of State Legislatures 2022). Leveraging provincial law may prove to be an optimal deterrent measure where national laws are unwieldy or controversial, such

as with the CFAA's history. In the future, provinces might also use the charging of suspected international cyberattackers – and, importantly, the publicization of such charges – to assert their provincial-level interests among the global order. James O. Goldsborough, writing in *Foreign Affairs* in 1993, pointed out that the U.S. province of California could be said to have its own foreign policy interests (Goldsborough 1993). Given that classical CDT posits that taking protective action under the criminal law is a marker of statehood, even provinces might be able to use domestic criminal charges not only to set global norms, but also to establish status and prestige among the social hierarchy of the international community.

Another interesting direction for future research regards testing whether, as I have implicitly assumed, publicized § 1030 bare indictments will achieve similar deterrent effects when they are issued against foreign nationals who are *not* nationals of one of the four countries that the U.S. government considers to be its nation-state cyber adversaries. Such bare indictments do exist. For example, in the REvil case study, a separate § 1030 bare indictment was issued against a Ukrainian national (DOJ OPA, November 08, 2021); pursuant to the indictment, this individual was extradited to face trial in the U.S. after having been apprehended in Poland (DOJ OPA, March 09, 2022). If a country such as Ukraine arguably has a friendly, allied, or non-adversarial relationship with the U.S., might the country be more likely to take offense to the issuance of a U.S. bare indictment – as though it were an 'unjustified' attack to national face – and therefore undermine the deterrent effect of a bare indictment by protecting its own nationals? Do bare indictments only achieve deterrent effects against cyberattacks if, as a prerequisite, the government of

the country from which the indicted individual hails is itself engaged in cyberattacking behavior adversarial to the indictment's issuer?

My project has focused on why bare indictments can deter cyberattacks *once bare indictments are issued against suspected cyberattackers*, and has devoted relatively less attention to what determines whether a bare indictment is issued at all. Thus, a third direction for future research is verifying whether any subset of suspected cyberattackers who hail from one of the four cyber adversary countries has been systematically excluded from being indicted, even though there would otherwise be enough evidence to issue a § 1030 bare indictment against these suspected cyberattackers. Are there any characteristics that tend to make a suspected cyberattacker from China, North Korea, Iran, or Russia less likely to be indicted? To what extent might a misconception that 'bare indictments cannot deter cyberattacks' have affected U.S. federal prosecutors' willingness to issue § 1030 bare indictments?

In any case, the U.S.'s usage of bare indictments to unilaterally assert international norms against cyberattacks may clarify standing U.S. policy practice as well as inform the policy practices of foreign nations. The insights generated from this project should be of interest to many fields of study, including sociology, behavioral science, political science, public policy, and law. This common interest means that the disciplines have much to learn from one another's perspectives; this rings especially true with respect to the potential harmonization between CDT and SDT. In 2004, Freedman wrote that the bridging the divide between the study of deterrence in criminology and the study of deterrence in international relations could be reciprocally beneficial for both branches, yet the formation

of the bridge had not come to pass; "What is striking is how similar the debates are in the strategic studies and criminological communities, yet how little they draw upon each others' work" (Freedman 2004, 60). Freedman compared criminal deterrence's emphasis on social norm formation with the norm-centric focuses of the English School and constructivism (2004, 68-69), which are two prevailing theoretical approaches in international relations (Bellamy 2007, 77). These theoretical approaches' conceptualization of interactions between nations as analogous to interactions in the social sphere may resonate with this project's focus on status, prestige, dominance, and face in the international community.

In an era of cyberwarfare and cyberattack-enabled hybrid warfare – which, per Hoffman's 2007 predictions, may use criminality as an instrument of international war – criminal deterrence's and state deterrence's ability and willingness to draw cross-disciplinary insights from one another has become not only a point of theoretical resonance, but also a practical necessity. The theoretical resonance between these branches of deterrence studies is a foundation for their potential to provide policy solutions to deterring cyberattack-enabled warfare that has gone from theory to actuality. Rarely, if ever, do the principles of CDT yield any insight that directly conflicts with the principles of SDT or vice versa; the relationship between these two theoretical branches is not confrontational, as they have the potential to be mutually reinforcing. In hybrid warfare, wherein domestic crime intersects with interstate war, the principles of criminal deterrence can speak to formulating both the target nation's deterrent actions and the international community's extended deterrent response.

When addressing the threat of cyberattacks, the necessity of integrating cross-disciplinary perspectives and approaches has gradually been recognized by the U.S. government, as discussed in Section 7.7. and as quoted by M. Mitchell Waldrop in a 2016 article for *Nature*: "'We've had too many computer scientists looking at cybersecurity, and not enough psychologists, economists, and human-factors people,' says Douglas Maughan, head of cybersecurity research at the U.S. Department of Homeland Security" (Waldrop 2016, 165). Notwithstanding their ability to use computerized means to carry out their offenses, cyberattackers – whether state actors or non-state actors – can be influenced in accordance with criminal deterrence theory.

Moreover, deterring individual actors can achieve deterrence at the nation-state level. As predicted by attribution theory and in accordance with the principle of *respondeat superior*, an attack on the face of these individuals can, when made common knowledge, become an imputed attack against the face of their states in the social hierarchy of the international community. This shows that the introduction of criminal deterrence principles and approaches should never be at the expense of disregarding the principles and approaches of international relations. To give another example, the analysis of status-seeking criminal motives and the suggestions for policy practitioners would be incoherent if this project were not to analyze foreign policy in determining what a particular state conceives of as markers of prestige. The behavioral analysis method of determining motive, a method drawn from criminology, would likewise be incomplete as applied in this context unless it were to take account of what international relations scholars have argued is a common motivation for state behavior.

Correspondingly, an overarching theme in this project on transnational cyberattacks has been the idea of going beyond boundaries. Just as cyberattacks transcend national, jurisdictional, and conceptual boundaries, so the arguably artificial boundaries between scholarly disciplines must become permeable in order to effectively counter this pressing threat in a global future. Whether cyberattacks are better categorized as criminal actions or as acts of war, both the study of crime and the study of warfare can speak to how cyberattacks might most effectively be deterred. Lest theorists make arguments that are unrealistic, or practitioners inadvertently undermine their own policy objectives, theory and praxis must unite to accomplish the mission of deterring cyberattacks.

As interstate wars have been initiated – and continue to be fought – over status, deterrence is accomplished by making common knowledge the denial of the face that these states seek. The issuance and publicization of bare indictments mobilizes the results of technical attribution into an attack on face; naming and shaming cannot deter shameless, anonymous cyberattackers unless such a measure not only unmasks them but also becomes a public accusation of criminality against these individuals and – where applicable – their state sponsors. The PLA Unit 61398 case study showed that unilateral assertions of global norms can arguably be far more effective than bilateral agreements to the same effect, and that keeping the international peace can be furthered through the exercise of domestic criminal law.

With the onset of hybrid warfare that melds domestic crime with international war, the impetus for the harmonization of CDT with SDT has become more pressing than ever before. Amidst a global future wherein cyber criminality's usage as an instrument of

international warfare has moved from theory to actuality, achieving deterrence against cyberattacks requires transcending boundaries in preparation for successfully facing the faceless adversaries.

BIBLIOGRAPHY

Acemoglu, Daron, and Matthew O. Jackson. "Social norms and the enforcement of laws." *Journal of the European Economic Association* 15, no. 2 (2017): 245-295.

Adams, Michael. "Why the OPM Hack is Far Worse than You Imagine." *Lawfare*, March 11, 2016. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

AFP. "Iran slams US sanctions over hacking scheme." *Times of Israel,* March 24, 2018. https://www.timesofisrael.com/iran-slams-us-sanctions-over-hacking-scheme/.

Aiesi, Matthew J., and Amanda L. Minikus. "The Rules of Engagement Are the Wrong Lexicon for Deterrence Signaling." *Lawfare,* June 09, 2020. https://www.lawfareblog.com/rules-engagement-are-wrong-lexicon-deterrence-signaling.

Aitel, Dave. "The Folly of 'Naming and Shaming' Iran." *Lawfare,* April 19, 2016. https://www.lawfareblog.com/folly-naming-and-shaming-iran.

Ajili, Hadi, and Mahsa Rouhi. "Iran's military strategy." *Survival* 61, no. 6 (2019): 139-152.

Alonso-Trabanco, Jose Miguel. "Understanding the 'Shiite Crescent' as Iranian Grand Strategy." *Geopolitical Monitor,* February 07, 2022. https://www.geopoliticalmonitor.com/understanding-the-shiite-crescent-as-iranian-grand-strategy/.

American Bar Association. "Rule 3.3: Candor Toward the Tribunal." *Model Rules of Professional Conduct,* August 2020. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_3_3_candor_toward_the_tribunal/.

Anderson, Linda S., Theodore G. Chiricos, and Gordon P. Waldo. "Formal and informal sanctions: A comparison of deterrent effects." *Social problems* 25, no. 1 (1977): 103-114.

Armitage, Susan. "When It Comes To Extraditions, Russia Often Cooperates." *NPR*, July 27, 2013. https://www.npr.org/sections/parallels/2013/07/27/205795904/when-it-comes-to-extraditions-russia-often-cooperates.

Arneson, Richard J. "Just Warfare Theory and Noncombatant Immunity." *Cornell Int'l LJ* 39 (2006): 663.

Aslam, Aqib, and Alpa Shah. *Tec (h) tonic Shifts: Taxing the "Digital Economy."* International Monetary Fund, 2020.

Ax, Joseph. “Russian sentenced to four-and-a-half years in U.S. prison for 'Citadel' malware.” *Reuters,* September 29, 2015. https://www.reuters.com/article/us-usa-cybersecurity-citadel/russian-sentenced-to-four-and-a-half-years-in-u-s-prison-for-citadel-malware-idUSKCN0RT2H320150929.

Barr, William P. “Attorney General William P. Barr Announces Indictment of Four Members of China’s Military for Hacking into Equifax.” *U.S. Department of Justice,* transcript of speech delivered in Washington, D.C., February 10, 2020. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

Barrett, Brian. “DOJ Indicts Hackers for Ransomware That Crippled Atlanta.” *Wired*, November 28, 2018. https://www.wired.com/story/doj-indicts-hackers-samsam-ransomware/.

Barrett, Brian. “How China’s Elite Hackers Stole the World’s Most Valuable Secrets.” *Wired*, December 20, 2018. https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/.

BBC News. “US justice department charges Chinese with hacking.” *BBC News*, May 19, 2014. https://www.bbc.com/news/world-us-canada-27475324.

Beccaria, Cesare. *Dei delitti e delle pene*, ed. Renato Fabietti. Milan: Ugo Mursia Editore, (1764a) 1973. http://www.letteraturaitaliana.net/pdf/Volume_7/t157.pdf.

Beccaria, Cesare. *On Crimes and Punishments* (Dei delitti e delle pene), trans. Edward D. Ingraham. Federalist Papers, 1764b. https://www.thefederalistpapers.org/wp-content/uploads/2013/01/Cesare-Beccaria-On-Crimes-and-Punishment.pdf.

Becker, Gary S. "Crime and punishment: An economic approach." In *The economic dimensions of crime*, pp. 13-68. London: Palgrave Macmillan, 1968.

Bedi, Monu. "Contract Breaches and the Criminal/Civil Divide: An Inter-Common Law Analysis." *Ga. St. UL Rev.* 28 (2013): 559.

Bellamy, Alex J. "The English School." In *International Relations Theory for the Twenty-First Century: An Introduction*, edited by Martin Griffiths (2007): 75-87.

Bénabou, Roland, and Jean Tirole. "Incentives and prosocial behavior." *American economic review* 96, no. 5 (2006): 1652-1678.

Bentham, Jeremy. *Introduction to the Principles of Morals and Legislation*. Oxford: Clarendon, (1789) 1823.

Bentham, Jeremy. *Rationale of Punishment.* London: Robert Heward, 1830.

Bentham, Jeremy. *Theory of Legislation*. Translated by Robert Hildreth and Etienne Dumont. London: Trubner, 1871.

Berge, Wendell. "Criminal Jurisdiction and the Territorial Principle." *Mich. L. Rev.* 30 (1931): 238.

Bertrand, Natasha. "Notorious Russian hacker was nabbed in the Maldives and extradited over 8,800 miles." *Business Insider,* March 11, 2015. https://www.businessinsider.com/notorious-russian-hacker-kidnapped-by-us-was-nabbed-in-the-maldives-2015-3.

Bilych, Ivanna, Alexander Gudko, Kateryna Kuntsevich, Matheus Sena, Malvika Seth, and Olena Sharvan. "Crisis in Ukraine: Its Legal Dimensions." *Razom,* April 14, 2014. https://www.razomforukraine.org/wp-content/uploads/2016/05/The-Crisis-in-Ukraine-Its-Legal-Dimensions.pdf.

Blake, Andrew. "Yu Pingan, Chinese national, arrested on charges linked to OPM, Anthem hacks." *Washington Times*, August 25, 2017. https://www.washingtontimes.com/news/2017/aug/25/yu-pingan-chinese-national-arrested-charges-linked/.

Blinder, Alan, Julie Turkewitz, and Adam Goldman. "Isolated and Adrift, an American Woman Turned Toward Iran." *New York Times,* February 16, 2019. https://www.nytimes.com/2019/02/16/us/monica-witt-iran.html.

Borghard, Erica D., and Shawn W. Lonergan. "Deterrence by denial in cyberspace." *Journal of Strategic Studies* (2021): 1-36.

Bossler, Adam M. "Perceived formal and informal sanctions on the willingness to commit cyber attacks against domestic and foreign targets." Journal of Crime and Justice 42, no. 5 (2019): 599-615.

Brantly, Aaron F. "The cyber deterrence problem." In *2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 31-54. IEEE, 2018.

Brown, Rufus, Van Ta, Douglas Bienstock, Geoff Ackerman, and John Wolfram. "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments." *Mandiant*, March 08, 2022. https://www.mandiant.com/resources/apt41-us-state-governments.

Brumfiel, Geoff, and David Welna. "Satellite Photos Reveal Extent Of Damage From Iranian Strike On Air Base In Iraq." *NPR,* January 08, 2020. https://www.npr.org/2020/01/08/794517031/satellite-photos-reveal-extent-of-damage-at-al-assad-air-base.

Burgess, Christopher. "Profile of a Traitor: How Monica Witt Proffered Herself to Iranian Intelligence." *ClearanceJobs,* February 15, 2019.

https://news.clearancejobs.com/2019/02/15/profile-of-a-traitor-how-monica-witt-proffered-herself-to-iranian-intelligence/.

Burgess, Matt. "The Quiet Way Advertisers are Tracking Your Browsing." *Wired,* February 26, 2022. https://www.wired.com/story/browser-fingerprinting-tracking-explained/.

Burgess, Matt. "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory." *Wired,* February 27, 2022. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

Burkhalter, Dorian. "When is a cyberattack a war crime?" *Swiss Info,* May 04, 2022. https://www.swissinfo.ch/eng/when-is-a-cyberattack-a-war-crime-/47556410.

Burt, Callie H., and Ronald L. Simons. "Self-control, thrill seeking, and crime: Motivation matters." *Criminal Justice and Behavior* 40, no. 11 (2013): 1326-1348.

Cain, Geoffrey. "Volodymyr Zelensky on War, Technology, and the Future of Ukraine." *Wired,* June 02, 2022. https://www.wired.com/story/volodymyr-zelensky-q-and-a-ukraine-war-technology/.

Carlin, John. "Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector." *U.S. Department of Justice,* transcript of speech delivered in Washington, D.C., March 24, 2016. https://www.justice.gov/opa/speech/assistant-attorney-general-john-p-carlin-delivers-remarks-press-conference-announcing.

Carmack, Dustin. "What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast." *Heritage Foundation,* May 20, 2021. https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc.

Casey, Joseph, and Katherine Koleski. "Backgrounder: China's 12th five-year plan." *US-China Economic and Security Review Commission*, June 24, 2011. https://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf.

Chalfant, Morgan. "Biden administration says Russia arrested Colonial Pipeline hacker." *The Hill*, January 14, 2022. https://thehill.com/homenews/administration/589850-biden-administration-says-russia-arrested-colonial-pipeline-hacker/.

Chalfin, Aaron, and Justin McCrary. "Criminal deterrence: A review of the literature." *Journal of Economic Literature* 55, no. 1 (2017): 5-48.

Chappell, Bill. “What We Know: Iran's Missile Strike Against The U.S. In Iraq.” *NPR,* January 08, 2020. https://www.npr.org/2020/01/08/794501068/what-we-know-irans-missile-strike-against-the-u-s-in-iraq.

Cheng, Joey T. "Dominance, prestige, and the role of leveling in human social hierarchy and equality." *Current opinion in psychology* 33 (2020): 238-244.

Cheng, Joey T., and Jessica L. Tracy. "The impact of wealth on prestige and dominance rank relationships." *Psychological Inquiry* 24, no. 2 (2013): 102-108.

China’s National People’s Congress. “12th Five-Year Plan (2011-2015) for National Economic and Social Development (EN).” *Asian and Pacific Energy Forum*, 2011. https://policy.asiapacificenergy.org/sites/default/files/12th%20Five-Year%20Plan%20%282011-2015%29%20for%20National%20Economic%20and%20Social%20Development%20%28EN%29.pdf.

Chiu, Elaine M. "The Challenge of Motive in the Criminal law." *Buffalo Criminal Law Review* 8, no. 2 (2005): 653-729.

Chwe, Michael Suk-Young. *Rational Ritual*. Princeton: Princeton University Press, 2001.

Clarke, Richard Alan, and Robert K. Knake. *Cyber war*. Old Saybrook: Tantor Media, Incorporated, 2014.

Cloudflare. “How to DDoS.” *Cloudflare*, n.d. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/.

Coats, Daniel R. “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community.” *ODNI,* February 13, 2018. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

Collier, Kevin. “Colonial pipeline hack claimed by Russian group DarkSide spurs emergency order from White House.” *NBC News,* May 10, 2021. https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878.

Council on Foreign Relations. “Denial of service attacks against U.S. banks in 2012–2013.” *Council on Foreign Relations,* n.d. https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013.

Criminal Complaint, *U.S. v. Park Jin Hyok*, Case No. MJ 18-1479 (C.D. Cal.). https://www.justice.gov/opa/press-release/file/1092091/download.

Criminal Complaint, *U.S. v. Su Bin*, Case No. 14-1318M (C.D. Cal.). https://www.exportlawblog.com/docs/us_v_su_complaint.pdf.

Criminal Complaint, *U.S. v. Yu Pingan*, Case 3:17-mj-02970-BGS (S.D. Cal.). https://www.politico.com/f/?id=0000015e-161b-df04-a5df-963f36840001.

Crown Prosecution Service. "Charging (The Director's Guidance) – sixth edition, December 2020." *CPS*, 2020. https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/Directors-Guidance-on-Charging-6th-Edition.pdf.

Cyberspace Solarium Commission. "Report." *Solarium,* March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

de Waal-Andrews, Wendy, Aiden P. Gregg, and Joris Lammers. "When status is grabbed and when status is granted: Getting ahead in dominance and prestige hierarchies." *British Journal of Social Psychology* 54, no. 3 (2015): 445-464.

Doyle, Charles. "Extraterritorial Application of American Criminal Law." *Congressional Research Service*, October 31, 2016. https://sgp.fas.org/crs/misc/94-166.pdf.

Drezner, Daniel W. "The hidden hand of economic coercion." *International Organization* 57, no. 3 (2003): 643-659.

Ducheine, Paul, and Peter Pijpers. "The Missing Component in Deterrence Theory: The Legal Framework." In *NL ARMS Netherlands Annual Review of Military Studies 2020*, pp. 475-500. TMC Asser Press, The Hague, 2021.

Dugas, Mari. "The Latest North Korea Cyber Indictment Should Serve as a Model." *Just Security*, February 24, 2021. https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/.

Duignan, Brian. "What Is the Difference Between Criminal Law and Civil Law?" *Encyclopedia Britannica*, n.d. https://www.britannica.com/story/what-is-the-difference-between-criminal-law-and-civil-law.

Egan, Lauren. "Ukrainians see their culture being erased as Russia hits beloved sites." *NBC News,* May 30, 2022. https://www.nbcnews.com/news/world/ukrainian-culture-erased-russia-hits-beloved-sites-rcna29972.

Electronic Frontier Foundation. "Computer Fraud And Abuse Act Reform." *EFF*, n.d. https://www.eff.org/issues/cfaa.

Erickson, Andrew. "Make China Great Again: Xi's Truly Grand Strategy." *War on the Rocks,* October 30, 2019. https://warontherocks.com/2019/10/make-china-great-again-xis-truly-grand-strategy/.

Farley, Robert. "Did the Obama-Xi Cyber Agreement Work?" *The Diplomat*, August 11, 2018. https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/.

FBI Newark. "#FugitiveFriday Help us find Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi, who are wanted for allegedly launching SamSam ransomware in the United States and other countries. http://ow.ly/R5J450zHdZd." *Twitter*, February 26, 2021. https://twitter.com/fbinewark/status/1365331467614707716.

Federal Bureau of Investigation. "A Brief Description of the Federal Criminal Justice Process." *FBI Resources: Victim Services*, n.d. https://www.fbi.gov/resources/victim-services/a-brief-description-of-the-federal-criminal-justice-process.

Federal Bureau of Investigation. "Combating the Iranian Cyber Threat." *FBI*, September 18, 2020. https://www.fbi.gov/news/stories/iran-at-center-of-cyber-crime-charges-in-three-cases-091820.

Federal Bureau of Investigation. "FBI Statement on Compromise of Colonial Pipeline Networks." *FBI*, May 10, 2021. https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks.

Federal Bureau of Investigation. "FBI Strategy Addresses Evolving Cyber Threat." *FBI*, September 16, 2020. https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620.

Federal Bureau of Investigation. "Private Industry Notification." *FBI*, January 26, 2022. https://www.ic3.gov/Media/News/2022/220126.pdf.

Federal Bureau of Investigation. "Ransomware Suspects Indicted." *FBI,* November 28, 2018. https://www.fbi.gov/news/stories/iranian-ransomware-suspects-indicted-112818.

Federal Judicial Center. "Sealed Cases in Federal Courts." *United States Courts,* October 23, 2009. https://www.uscourts.gov/sites/default/files/sealed-cases.pdf.

Fincham, Frank D., and Joseph M. Jaspars. "Attribution of responsibility: From man the scientist to man as lawyer." *Advances in experimental social psychology* 13 (1980): 81-138.

Finkle, Jim. "Mandiant goes viral after China hacking report." *Reuters,* February 22, 2013. https://www.reuters.com/article/net-us-hackers-virus-china-mandiant/mandiant-goes-viral-after-china-hacking-report-idUSBRE91M02P20130223.

Finn, Peter. "Decades of distrust restrain cooperation between FBI and Russia's FSB." *Washington Post,* May 08, 2013. https://www.washingtonpost.com/world/national-security/decades-of-distrust-restrain-cooperation-between-fbi-and-russias-fsb/2013/05/08/584f1888-b7f3-11e2-b94c-b684dda07add_story.html.

Foreign, Commonwealth & Development Office. "UK and allies hold Chinese state responsible for pervasive pattern of hacking." *GOV.UK,* July 19, 2021.

https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking.

Fortinet. “Distributed Denial-of-Service (DDoS) Attacks Meaning and Prevention.” *Fortinet Cyberglossary,* 2022. https://www.fortinet.com/resources/cyberglossary/ddos-attack.

Freedman, Lawrence. "Deterrence: A reply." *Journal of Strategic Studies* 28, no. 5 (2005): 789-801.

Freedman, Lawrence. *Deterrence*. Cambridge: Polity Press, 2004.

George, Alexander L., and Richard Smoke. *Deterrence in American foreign policy: Theory and practice*. Columbia University Press, 1974.

Glaser, Charles L. "Political consequences of military strategy: Expanding and refining the spiral and deterrence models." *World politics* 44, no. 4 (1992): 497-538.

Goldsborough, James O. “California’s Foreign Policy.” *Foreign Affairs,* Spring 1993. https://www.foreignaffairs.com/articles/united-states/1993-03-01/californias-foreign-policy.

Goldsmith, Jack, and Robert D. Williams. “The Failure of the United States’ Chinese-Hacking Indictment Strategy.” *Lawfare*, December 28, 2018. https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

Goldsmith, Jack. “The Puzzle of the GRU Indictment.” *Lawfare*, October 21, 2020. https://www.lawfareblog.com/puzzle-gru-indictment.

Goldsmith, Jack. “U.S. Attribution of China’s Cyber-Theft Aids Xi’s Centralization and Anti-Corruption Efforts.” *Lawfare*, June 21, 2016. https://www.lawfareblog.com/us-attribution-chinas-cyber-theft-aids-xis-centralization-and-anti-corruption-efforts.

Goldsmith, Jack. “Why Did DOJ Indict the Chinese Military Officers?” *Lawfare*, May 20, 2014. https://www.lawfareblog.com/why-did-doj-indict-chinese-military-officers.

Goodman, Will. "Cyber deterrence: Tougher in theory than in practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-135.

Gouvea, Julia. "Insights from small-N studies." *CBE—Life Sciences Education* 16, no. 3 (2017): 1-4.

Graff, Garrett M. “How the US Forced China to Quit Stealing—Using a Chinese Spy.” *Wired*, October 11, 2018. https://www.wired.com/story/us-china-cybertheft-su-bin/.

Green, James A. "Introduction." In *Cyber Warfare*, edited by James A. Green, pp. 1-6. London: Routledge, 2015a.

Green, James A. "The regulation of cyber warfare under the *jus ad bellum*." In *Cyber Warfare*, edited by James A. Green, pp. 96-124. London: Routledge, 2015b.

Greenberg, Andy. "China Tests The Limits of Its US Hacking Truce." *Wired*, October 31, 2017. https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/.

Greenberg, Andy. "Facebook Catches Iranian Spies Catfishing US Military Targets." *Wired*, July 15, 2021. https://www.wired.com/story/facebook-iran-espionage-catfishing-us-military/.

Greenberg, Andy. "North Korea's Sloppy, Chaotic Cyberattacks Also Make Perfect Sense." *Wired*, June 15, 2017. https://www.wired.com/story/north-korea-cyberattacks/.

Greenberg, Andy. "Obama Curbed Chinese Hacking, But Russia Won't Be So Easy." *Wired,* December 16, 2016. https://www.wired.com/2016/12/obama-russia-hacking-sanctions-china/.

Greenberg, Andy. "The Case for War Crimes Charges Against Russia's Sandworm Hackers." *Wired,* May 12, 2022. https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/.

Greenberg, Andy. "The WIRED Guide to Cyberwar." *Wired*, August 23, 2019. https://www.wired.com/story/cyberwar-guide/.

Greig, Jonathan. "White House confirms person behind Colonial Pipeline ransomware attack nabbed during Russian REvil raid." *ZDNet,* January 14, 2022. https://www.zdnet.com/article/white-house-says-person-behind-colonial-pipeline-ransomware-attack-nabbed-during-russian-raid/.

Haass, Richard N. "Economic Sanctions: Too Much of a Bad Thing." *Brookings*, June 01, 1998. https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/.

Hamilton, V. Lee. "Chains of Command: Responsibility Attribution in Hierarchies." *Journal of Applied Social Psychology* 16, no. 2 (1986): 118-138.

Hardie, John. "Biden Administration Targets Corruption in Ukraine's Judiciary." *FDD,* December 16, 2021. https://www.fdd.org/analysis/2021/12/17/corruption-in-ukraines-judiciary/.

Harding, Luke. "Russian law prevents extradition." *Guardian*, May 22, 2007. https://www.theguardian.com/world/2007/may/22/russia.lukeharding.

Harold, Scott W. "The U.S.-China Cyber Agreement: A Good First Step." *The RAND Blog*, August 01, 2016. https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.

Hart, Herbert Lionel Adolphus. *Essays on Bentham: Jurisprudence and political philosophy*. OUP Oxford, 1982.

Healey, Jason. "The spectrum of national responsibility for cyberattacks." *The Brown Journal of World Affairs* 18, no. 1 (2011): 57-70.

Hechler, David. "What Is the Point of These Nation-State Indictments?" *Lawfare*, February 08, 2021. https://www.lawfareblog.com/what-point-these-nation-state-indictments.

Hendriks, Marcus Solarz. "Iran Wants Leverage, Not a Nuke (For Now)." *National Interest*, May 10, 2021. https://nationalinterest.org/blog/buzz/iran-wants-leverage-not-nuke-now-184790.

Hessick, Carissa Byrne. "Motive's role in criminal punishment." *S. Cal. L. Rev*. 80 (2006): 89.

Hinck, Garrett, and Tim Maurer. "Persistent enforcement: criminal charges as a response to nation-state malicious cyber activity." *J. Nat'l Sec. L. & Pol'y* 10 (2020): 525-561.

Hinck, Garrett, and Tim Maurer. "What's the Point of Charging Foreign State-Linked Hackers?" *Lawfare*, May 24, 2019. https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers.

Ho, David Yau-fai. "On the concept of face." *American journal of sociology* 81, no. 4 (1976): 867-884.

Hoffman, Frank G. *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies, 2007.

Hofmann, Frank. "The hybrid war that began before Russia invaded Ukraine." *DW*, February 25, 2022. https://www.dw.com/en/hybrid-war-in-ukraine-began-before-russian-invasion/a-60914988.

Holt, Thomas J. "Computer hacking and the hacker subculture." *The palgrave handbook of international cybercrime and cyberdeviance* (2020): 725-742.

Iasiello, Emilio. "Cyber attack: A dull tool to shape foreign policy." In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pp. 1-18. IEEE, 2013.

Iasiello, Emilio. "Is cyber deterrence an illusory course of action?." *Journal of Strategic Security* 7, no. 1 (2014): 54-67.

Indictment, *U.S. v. Ajily*, Case 2:15-cr-00015-wks (D. Vt.). https://www.justice.gov/opa/press-release/file/982106/download.

Indictment, *U.S. v. Akulov*, Case No. 21-20047-HLT/JPC (D. Kan.). https://www.justice.gov/opa/press-release/file/1486836/download.

Indictment, *U.S. v. Andrienko,* Criminal No. 20-316 (W.D. Pa.). https://www.justice.gov/opa/page/file/1098481/download.

Indictment, *U.S. v. Ding Xiaoyang*, Case No. 21 CR1622 GPC (S.D. Cal.). https://www.justice.gov/opa/press-release/file/1412916/download.

Indictment, *U.S. v. Dokuchaev,* CR 17 103 (N.D. Cal.). https://www.justice.gov/opa/press-release/file/948201/download.

Indictment, *U.S. v. Fathi,* 16 Crim 48 (S.D.N.Y.). https://www.justice.gov/usao-sdny/file/835061/download.

Indictment, *U.S. v. Gladkikh*, Case 1:21-cr-00442-CJN (D.D.C.). https://www.justice.gov/opa/press-release/file/1486831/download.

Indictment, *U.S. v. Jon,* CR 2:20-cr-00614-DMG (C.D. Cal.). https://www.justice.gov/opa/press-release/file/1367701/download.

Indictment, *U.S. v. Kazemi*, 21 Crim 644 (S.D.N.Y.). https://www.justice.gov/usao-sdny/press-release/file/1449276/download.

Indictment, *U.S. v. Li Xiaoyu,* 4:20-CR-6019-SMJ (E.D. Wash.). https://www.justice.gov/opa/press-release/file/1295981/download.

Indictment, *U.S. v. Morenets,* Case 2:18-cr-00263-MRH (W.D. Pa.). https://www.justice.gov/opa/page/file/1098481/download.

Indictment, *U.S. v. Netyksho,* Case 1:18-cr-00215-ABJ (D.D.C.). https://www.justice.gov/file/1080281/download.

Indictment, *U.S. v. Polyanin*, Criminal No. 3-21CR0393-B (N.D. Tex.). https://www.justice.gov/opa/press-release/file/1447121/download.

Indictment, *U.S. v. Rafatnejad*, 18 Crim 94 (S.D.N.Y.). https://www.justice.gov/usao-sdny/press-release/file/1045781/download.

Indictment, *U.S. v. Savandi*, Criminal No. 18-CR-704(BRM) (D.N.J.). https://www.justice.gov/opa/press-release/file/1114741/download.

Indictment, *U.S. v. Wang Dong*, Criminal No. 14-118 (W.D. Pa). https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

Indictment, *U.S. v. Wang Fujie,* Case 1:19-cr-00153-JRS-MJD (S.D. Ind.). https://www.justice.gov/opa/press-release/file/1161466/download.

Indictment, *U.S. v. Witt*, Case No. 1:19-cr-4 (D.D.C.). https://www.justice.gov/opa/press-release/file/1131726/download.

Indictment, *U.S. v. Wu Yingzhuo*, Criminal No. 17-247 (W.D. Pa.). https://www.justice.gov/opa/press-release/file/1013866/download.

Indictment, *U.S. v. Wu Zhiyong*, No. 2:20-CD046 [stamp illegible] (N.D. Ga.). https://www.justice.gov/opa/press-release/file/1246891/download.

Indictment, *U.S. v. Zhang Zhang-Gui*, Case No. 13CR3132-H (S.D. Cal.). https://www.justice.gov/opa/press-release/file/1106491/download.

Indictment, *U.S. v. Zhu Hua*, 18 Crim 891 (S.D.N.Y.). https://www.justice.gov/opa/press-release/file/1121706/download.

Insikt Group. "Iran-Linked Threat Actor The MABNA Institute's Operations in 2020." *Recorded Future,* April 21, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0421.pdf.

International Committee of the Red Cross. "Self-defence." *How Does Law Protect In War?,* 2022. https://casebook.icrc.org/glossary/self-defence.

Iran Primer. "U.S. Sanctions Iran for Election Hacking." *United States Institute of Peace*, November 19, 2021. https://iranprimer.usip.org/blog/2021/nov/18/us-sanctions-iran-election-hacking.

Jacobs, Bruce A., Volkan Topalli, and Richard Wright. "Managing retaliation: Drug robbery and informal sanction threats." *Criminology* 38, no. 1 (2000): 171-198.

Jacobs, John G.L.J., and Martijn W.M. Kitzen. "Hybrid Warfare." *Oxford Bibliographies: International Relations*, September 22, 2021. https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0050.xml.

Japan National Diet. "Code of Criminal Procedure (Act No. 131 of 1948)." *Japanese Law Translation,* August 25, 2021. https://www.japaneselawtranslation.go.jp/en/laws/view/2056/en.

Jensen, Eric Talbot. "Cyber deterrence." *Emory Int'l L. Rev*. 26 (2012): 773.

Jervis, Robert. "Why nuclear superiority doesn't matter." *Political Science Quarterly* 94, no. 4 (1979): 617-633.

Jones, Randall S. "North Korean Economy Shrinks in 2020." *KEI*, October 01, 2021. https://keia.org/the-peninsula/north-korean-economy-shrinks-in-2020/.

Kakkar, Hemant, Niro Sivanathan, and Matthias S. Gobel. "Fall from grace: The role of dominance and prestige in the punishment of high-status actors." *Academy of Management Journal* 63, no. 2 (2020): 530-553.

Karelaia, Natalia, and Steffen Keck. "When deviant leaders are punished more than non-leaders: The role of deviance severity." *Journal of Experimental Social Psychology* 49, no. 5 (2013): 783-796.

Kassab, Hanna Samir. "In search of cyber stability: international relations, mutually assured destruction and the age of cyber warfare." In *Cyberspace and International Relations*, pp. 59-76. Springer, Berlin, Heidelberg, 2014.

Keitner, Chimène I. "Attribution by Indictment." *American Journal of International Law* 113 (2019): 207-212.

Kerner, Sean Michael. "Colonial Pipeline hack explained: Everything you need to know." *TechTarget,* April 26, 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Kerr, Orin. "The Supreme Court Reins In the CFAA in Van Buren." *Lawfare*, June 9, 2021. https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren.

Khong, Yuen Foong. "Power as prestige in world politics." *International Affairs* 95, no. 1 (2019): 119-142.

Knopf, Jeffrey W. "The fourth wave in deterrence research." *Contemporary Security Policy* 31, no. 1 (2010): 1-33.

Knutson, Jacob. "Colonial Pipeline hack: Gas shortage grips southeast U.S." *Axios,* May 12, 2021. https://www.axios.com/2021/05/12/gas-shortage-colonial-pipeline.

Koerner, Brendan. "When Can a Defendant Be Tried in Absentia?" *Slate*, June 19, 2003. https://slate.com/news-and-politics/2003/06/when-can-a-defendant-be-tried-in-absentia.html.

Krebs, Brian. "The Backstory Behind Carder Kingpin Roman Seleznev's Record 27 Year Prison Sentence." *Krebs on Security,* April 24, 2017. https://krebsonsecurity.com/2017/04/the-backstory-behind-carder-kingpin-roman-seleznevs-record-27-year-prison-sentence/.

Kushner, David. 26 February 2013. "The Real Story of Stuxnet." *IEEE Spectrum*, February 26, 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet.

Kydd, Andrew. "Game theory and the spiral model." *World Politics* 49, no. 3 (1997): 371-400.

Lacy, Dean, and Emerson MS Niou. "A theory of economic sanctions and issue linkage: The roles of preferences, information, and threats." *The journal of politics* 66, no. 1 (2004): 25-42.

Larson, Deborah Welch, and Alexei Shevchenko. *Quest for Status: Chinese and Russian Foreign Policy*. New Haven: Yale University Press, 2019.

Legal Information Institute. "Charge." *Cornell Law School Wex*, February 2022. https://www.law.cornell.edu/wex/charge.

Legal Information Institute. "Conviction." *Cornell Law School Wex*, n.d. https://www.law.cornell.edu/wex/conviction.

Legal Information Institute. "Efficient Breach." *Cornell Law School Wex*, n.d. https://www.law.cornell.edu/wex/efficient_breach.

Legal Information Institute. "Misdemeanor." *Cornell Law School Wex*, August 2021. https://www.law.cornell.edu/wex/misdemeanor.

Legal Information Institute. "Probable Cause." *Cornell Law School Wex*, n.d. https://www.law.cornell.edu/wex/probable_cause.

Leonard, David P. "Character and motive in evidence law." *Loy. L.A. L. Rev.* 34 (2001): 439.

Libicki, Martin C. *Cyberdeterrence and cyberwar*. RAND Corporation, 2009. https://apps.dtic.mil/sti/pdfs/ADA508151.pdf.

Lim, Kevjn. "Iran's Grand Strategic Logic." *Survival* 62, no. 5 (2020): 157-172.

Lin, Herb. "What the National Counterintelligence and Security Center Really Said About Chinese Economic Espionage." *Lawfare*, July 31, 2018. https://www.lawfareblog.com/what-national-counterintelligence-and-security-center-really-said-about-chinese-economic-espionage.

Little, William. *Introduction to Sociology – 2nd Canadian Edition.* BCcampus, 2006. https://opentextbc.ca/introductiontosociology2ndedition/.

Logan, Trevor, and Pavak Patel. "Data Visualization: U.S. Sanctions Against Malicious Cyber Actors." *Foundation for Defense of Democracies*, April 20, 2020a. https://www.fdd.org/analysis/visuals/2020/02/28/data-visualization%3A-us-sanctions-against-malicious-cyber-actors/.

Logan, Trevor, and Pavak Patel. "Washington Uses Sanctions and Indictments Inconsistently When Combating Malicious Cyber Activity." *Foundation for Defense of Democracies*, April 20, 2020b. https://www.fdd.org/analysis/2020/04/15/washington-uses-sanctions-and-indictments-inconsistently-when-combating-malicious-cyber-activity/.

Logan, Trevor. "U.S. Should Indict and Sanction Cyber Adversaries." *FDD,* February 27, 2019. https://www.fdd.org/analysis/2019/02/27/u-s-should-indict-and-sanction-cyber-adversaries/.

London Metropolitan Police. “CPS gives authority to charge man with sexual offences.” *Metropolitan Police*, May 26, 2022. https://news.met.police.uk/news/cps-gives-authority-to-charge-man-with-sexual-offences-448578.

Lonergan, Erica. “What Makes This Attribution of Chinese Hacking Different.” *Carnegie Endowment for International Peace*, July 22, 2021. https://carnegieendowment.org/2021/07/22/what-makes-this-attribution-of-chinese-hacking-different-pub-85023.

Lucas, Ryan. “Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?” *NPR*, February 05, 2019. https://www.npr.org/2019/02/05/691403968/charges-against-chinese-hackers-are-now-common-why-dont-they-deter-cyberattacks.

Lyngaas, Sean. “US officials believe Russia arrested hacker responsible for Colonial Pipeline attack.” *CNN,* January 14, 2022. https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest/index.html.

MacCormack, Anna. "United States, China, and Extradition: Ready for the Next Step." *NYUJ Legis. & Pub. Pol'y* 12 (2008): 445.

Machtiger, Peter. “Disrupt, Don’t Indict: Why the United States Should Stop Indicting Foreign State Actor Hackers.” *Just Security,* April 03, 2020. https://www.justsecurity.org/69104/disrupt-dont-indict-why-the-united-states-should-stop-indicting-foreign-state-actor-hackers/.

Machtiger, Peter. “The Latest GRU Indictment: A Failed Exercise in Deterrence.” *Just Security,* October 29, 2020. https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/.

Mandiant. “APT1: Exposing One of China's Cyber Espionage Units.” *Mandiant*, 2013. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.

Mandiant. “Red Line Drawn: China recalculates its use of cyber espionage.” *Mandiant*, June 2016. https://www.mandiant.com/sites/default/files/2021-09/rpt-china-espionage-1.pdf.

Maner, Jon K. "Dominance and prestige: A tale of two hierarchies." *Current Directions in Psychological Science* 26, no. 6 (2017): 526-531.

Mankoff, Jeffrey. “Russia’s War in Ukraine: Identity, History, and Conflict.” *Center for Strategic and International Studies*, April 22, 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220422_Mankoff_RussiaWar_Ukraine.pdf?tGhbfT.eyo9DdEsYZPaTWbTZUtGz9o2_.

Markey, Daniel. "Prestige and the origins of war: Returning to realism's roots." *Security studies* 8, no. 4 (1999): 126-172.

Markovits, Daniel, and Emad H. Atiq. "Philosophy of Contract Law." *Stanford Encyclopedia of Philosophy*, 2021. https://plato.stanford.edu/entries/contract-law/.

Marks, Joseph. "One year ago, Colonial Pipeline changed the cyber landscape forever." *Washington Post,* May 06, 2022. https://www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/.

Masters, Jonathan. "What is Extradition?" *Council on Foreign Relations,* January 28, 2020. https://www.cfr.org/backgrounder/what-extradition.

Matsueda, Ross L., Rosemary Gartner, Irving Piliavin, and Michael Polakowski. "The prestige of criminal and conventional occupations: A subcultural model of criminal activity." *American sociological review* (1992): 752-770.

Mazarr, Michael J. "Understanding Deterrence." In *NL ARMS Netherlands Annual Review of Military Studies 2020*, pp. 13-28. TMC Asser Press, The Hague, 2021.

McClanahan, Kaylene J., Jon K. Maner, and Joey T. Cheng. "Two ways to stay at the top: Prestige and dominance are both viable strategies for gaining and maintaining social rank over time." *Personality and Social Psychology Bulletin* (2021): 01461672211042319.

McGuinness, Damien. "How a cyber attack transformed Estonia." *BBC News*, April 27, 2017. https://www.bbc.com/news/39655415.

McKenzie, Timothy M. *Is Cyber Deterrence Possible?* Air University Press, 2017.

Mearsheimer, John J. *Conventional deterrence*. Ithaca: Cornell University Press, 1985.

Medina Falzone, Gabby. "Case Studies in Social Death: The Criminalization and Dehumanization of Six Black and Latino Boys." *The Urban Review* 54, no. 2 (2022): 233-254.

Memorandum, *U.S. v. Seleznev*, No. 17-30085, D.C. No. 2:11-cr-00070-RAJ-1 (9th Cir). https://www.courthousenews.com/wp-content/uploads/2019/04/Seleznev9CA.pdf.

Mercer, Jonathan. "The illusion of international prestige." *International Security* 41, no. 4 (2017): 133-168.

Microsoft Digital Security Unit. "An overview of Russia's cyberattack activity in Ukraine." *Microsoft*, April 27, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Miller, Maggie. “Russia arrests hacker in Colonial Pipeline attack, U.S. says.” *Politico*, January 14, 2022. https://www.politico.com/news/2022/01/14/russia-colonial-pipeline-arrest-527166.

Morgenstern, Oskar, and John Von Neumann. *Theory of games and economic behavior*. 3rd ed. Princeton: Princeton University Press, 1953.

Mosechkin, Ilya. "Why Women Kill: Studying Motives for Committing Crimes." *Women & Criminal Justice* (2021): 1-14.

Nagin, Daniel S. "Deterrence in the twenty-first century." *Crime and justice* 42, no. 1 (2013): 199-263.

Nakashima, Ellen, and William Wan, “U.S. announces first charges against foreign country in connection with cyberspying.” *Washington Post*, May 19, 2014. https://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

Nakashima, Ellen. “Following U.S. indictments, China shifts commercial hacking away from military to civilian agency.” *Washington Post,* November 30, 2015. https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html.

Nakashima, Ellen. “Hacks of OPM databases compromised 22.1 million people, federal authorities say.” *Washington Post*, July 09, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

Nakashima, Ellen. “Obama signs secret directive to help thwart cyberattacks.” *Washington Post,* November 14, 2012. https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

National Conference of State Legislatures. “Computer Crime Statutes.” *NCSL,* May 04, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

National Cyber Security Centre. “UK and allies hold Chinese state responsible for pervasive pattern of hacking.” *National Cyber Security Centre,* July 19, 2021. https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking.

Neufeld, Derrick J. "Understanding cybercrime." In *2010 43rd Hawaii International Conference on System Sciences*, pp. 1-10. IEEE, 2010.

Newman, Lily Hay. “Security News This Week: North Korea’s Lazarus Group Was Behind $540 Million Ronin Theft.” *Wired,* April 16, 2022. https://www.wired.com/story/ronin-hack-lazarus-tmobile-breach-data-malware-telegram/.

Nichols, Michelle. “North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report.” *Reuters,* August 05, 2019. https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

Nossel, Suzanne. “How to Help Ukraine Fight Cultural Erasure.” *Foreign Policy*, May 16, 2022. https://foreignpolicy.com/2022/05/16/ukraine-russia-fight-cultural-erasure/.

O’Harrow, Robert, and Barton Gellman. “Secret cyber directive calls for ability to attack without warning.” *Washington Post,* June 07, 2013. https://www.washingtonpost.com/world/national-security/secret-cyber-directive-calls-for-ability-to-attack-without-warning/2013/06/07/6a4cc762-cfc0-11e2-9f1a-1a7cdee20287_story.html.

O’Hear, Michael M. “Why Don’t We Punish People Who Kill in Self-Defense?” *Marquette University Law School Faculty Blog*, October 23, 2008. https://law.marquette.edu/facultyblog/2008/10/why-dont-we-punish-people-who-kill-in-self-defense/.

Office of the Director of National Intelligence. “Annual Threat Assessment of the U.S. Intelligence Community.” *ODNI,* February 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Oliver, DeJarvis, and Adriane B. Randolph. "Hacker Definitions in Information Systems Research." *Journal of Computer Information Systems* 62, no. 2 (2022): 397-409.

O'Neill, Barry. “Nuclear Weapons and National Prestige.” *Cowles Foundation Discussion Paper* No. 1560 (February 2006), https://cowles.yale.edu/sites/default/files/files/pub/d15/d1560.pdf.

Osborne, Charlie. “Colonial Pipeline ransomware attack: Everything you need to know.” *ZDNet,* May 13, 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/.

Osborne, Charlie. “DarkSide explained: The ransomware group responsible for Colonial Pipeline attack.” *ZDNet,* May 14, 2021. https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/.

Pal, Alasdair, and Mohamed Junayd. “Maldives shelters sanctioned Russian billionaires' yachts.” *Reuters,* April 07, 2022. https://www.reuters.com/world/maldives-shelters-sanctioned-russian-billionaires-yachts-2022-04-07/.

Perez, Evan, and Shimon Prokupecz. “First on CNN: U.S. data hack may be 4 times larger than the government originally said.” *CNN*, June 24, 2015. https://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.

Perkins, Rollin M. "The territorial principle in criminal law." *Hastings LJ* 22 (1970): 1155.

Petcu, Alina Georgiana. “SamSam Ransomware 101: How It Works and How to Avoid It.” *Heimdal Security*, December 31, 2020. https://heimdalsecurity.com/blog/samsam-ransomware/.

Peters, Allison, and Pierce MacConaghy. “Unpacking U.S. Cyber Sanctions.” *Third Way,* January 29, 2021. https://www.thirdway.org/memo/unpacking-us-cyber-sanctions.

Petherick, Wayne A., and Brent E. Turvey. "Criminal motivation." In *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, edited by Brent E. Turvey, 273-308. Burlington: Elsevier, 2008.

Plea Agreement, *U.S. v. Golestaneh,* Case 2:13-cr-00160-wks (D. Vt.). https://www.justice.gov/opa/file/796686/download.

Plea Agreement, *U.S. v. Su Bin*, No. 14-131 (C.D. Cal.). https://www.justice.gov/opa/file/834936/download.

Polman, Evan, Nathan C. Pettit, and Batia M. Wiesenfeld. "Effects of wrongdoer status on moral licensing." *Journal of Experimental Social Psychology* 49, no. 4 (2013): 614-623.

Powell, Robert. "Nuclear deterrence and the strategy of limited retaliation." *American Political Science Review* 83, no. 2 (1989): 503-519.

Pruitt, Ellen. “Indictments Don’t Deter Cyberattacks, So Why Does the U.S. Keep Using Them? An Analysis in Response to the U.S.’s Recent Indictment of Six Russian Hackers.” *University of Baltimore Law Review*, February 26, 2021. https://ubaltlawreview.com/2021/02/26/indictments-dont-deter-cyberattacks-so-why-does-the-u-s-keep-using-them-an-analysis-in-response-to-the-u-s-s-recent-indictment-of-six-russian-hackers/.

Qi, Xiaoying. "Face: A Chinese concept in a global sociology." *Journal of Sociology* 47, no. 3 (2011): 279-295.

Qin, Gang. “China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel.” *Ministry of Foreign Affairs of the People’s Republic of China*, May 20, 2020. https://www.mfa.gov.cn/ce/cegv/eng/fyrth/t1157520.htm.

Quackenbush, Stephen L. "Deterrence theory: where do we stand?" *Review of International Studies* 37, no. 2 (2011): 741-762.

RAND Corporation. "Cyber warfare." *RAND*, 2021. https://www.rand.org/topics/cyber-warfare.html.

Randall, Kenneth C. "Universal jurisdiction under international law." *Tex. L. Rev.* 66 (1987): 785.

Rapier, Robert. "Panic Buying Is Causing Fuel Shortages Along The Colonial Pipeline Route." *Forbes,* May 11, 2021. https://www.forbes.com/sites/rrapier/2021/05/11/panic-buying-is-causing-gas-shortages-along-the-colonial-pipeline-route/?sh=75d113d56b49.

Renshon, Jonathan. "Status deficits and war." *International Organization* 70, no. 3 (2016): 513-550.

Renshon, Jonathan. *Fighting for Status: Hierarchy and Conflict in World Politics*. Princeton: Princeton University Press, 2017.

Reuters Staff. "U.S. accuses China of violating bilateral anti-hacking deal." *Reuters,* November 08, 2018. https://www.reuters.com/article/ctech-us-usa-china-cyber-idCAKCN1NE02E-OCATC.

RFE/RL. "Western Diplomats Express Concern About Ukraine's Judicial Reforms After Delay." *RadioFreeEurope RadioLiberty,* September 17, 2021. https://www.rferl.org/a/ukraine-judicial-reform-delays/31463927.html.

Rogers, Lindsay. "Russians Oligarchs Are Being Allowed to Travel to Popular Tourist Destinations." *InsideHook*, March 16, 2022. https://www.insidehook.com/daily_brief/travel/russians-being-allowed-travel-popular-tourist-destinations.

Romo, Vanessa. "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack." *NPR,* May 11, 2021. https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack.

Rosen, Frederick. "Crime, punishment and liberty." *History of Political Thought* 20, no. 1 (1999): 173-185.

Rosenberg, Steven. "Russia cyber-plots: Dutch defend decision not to arrest suspects." *BBC News*, October 06, 2018. https://www.bbc.com/news/world-europe-45758316.

Rosenfeld, Richard. "The Social Construction of Crime." *Oxford Bibliographies: Criminology*, October 27, 2017. https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0050.xml.

Sabbagh, Dan, Jennifer Rankin, and Peter Walker. “UK and allies accuse Chinese state-backed group of Microsoft hack.” *Guardian*, July 19, 2021. https://www.theguardian.com/world/2021/jul/19/uk-allies-accuse-chinese-state-backed-group-microsoft-hack.

Scully, Diana, and Joseph Marolla. "Convicted rapists' vocabulary of motive: Excuses and justifications." *Social problems* 31, no. 5 (1984): 530-544.

Segal, Adam. “The U.S.-China Cyber Espionage Deal One Year Later.” *Council on Foreign Relations*, September 28, 2016. https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes, 2013.

Shinkman, Paul. “China Threatens U.S., Allies Following Claims of Cyber Hacks.” *U.S. News,* July 19, 2021. https://www.usnews.com/news/world-report/articles/2021-07-19/china-threatens-us-allies-following-claims-of-cyber-hacks-we-will-retaliate.

Shinkman, Paul. “Russia Denies Involvement in Darkside Attack on Colonial Pipeline.” *U.S. News,* May 11, 2021. https://www.usnews.com/news/world-report/articles/2021-05-11/russia-denies-involvement-in-darkside-attack-on-colonial-pipeline.

Shore, Jennifer. “Don’t Underestimate Ukraine’s Volunteer Hackers.” *Foreign Policy*, April 11, 2022. https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/.

Soldatov, Andrei, and Irina Borogan. “Can America's Spies Work With Russia's?” *Atlantic,* March 04, 2017. https://www.theatlantic.com/international/archive/2017/03/fsb-cia-russia/518589/.

Soldatov, Andrei. “Even amid the saber-rattling, Russia’s spies reach out to the U.S.” *Washington Post,* February 01, 2022. https://www.washingtonpost.com/opinions/2022/02/01/russia-fsb-power-ukraine/.

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*. Cambridge: Cambridge University Press, 2010.

Solis, Nathan. “Ninth Circuit Upholds 27-Year Sentence for Russian Hacker.” *Courthouse News Service*, April 02, 2019. https://www.courthousenews.com/ninth-circuit-upholds-27-year-sentence-for-russian-hacker/.

Solove, Daniel J. *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press, 2011.

Sophos. “SamSam: The (Almost) Six Million Dollar Ransomware.” *Sophos*, July 19, 2018. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf.

Sorin, Sylvain. "Bluff and reputation." In *Game Theory and Economic Analysis*. London, New York: Routledge (2002): 57-73.

Spiekermann-Hoff, Sarah, and Jana Korunovska. "Towards a Value Theory for Personal Data." *Working Papers on Information Systems, Information Business and Operations*. WU Vienna University of Economics and Business, Vienna (2016).

State Bar of California. “Rule 3.3 Candor Toward the Tribunal.” *State Bar of California*, n.d. https://www.calbar.ca.gov/Portals/0/documents/rules/Rule_3.3-Exec_Summary-Redline.pdf.

Stiennon, Richard. "A short history of cyber warfare." In *Cyber Warfare*, edited by James A. Green, pp. 7-32. London: Routledge, 2015.

Straub, Jeremy. "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios." *Technology in Society* 59 (2019): 101177.

Sunstein, Cass R., David Schkade, and Daniel Kahneman. "Do people want optimal deterrence?" *The Journal of Legal Studies* 29, no. 1 (2000): 237-253.

Sweijs, Tim, and Samuel Zilincik. "The Essence of Cross-Domain Deterrence." In *NL ARMS Netherlands Annual Review of Military Studies 2020*, pp. 129-158. TMC Asser Press, The Hague, 2021.

Thomas, Charles W., and Donna M. Bishop. "The effect of formal and informal sanctions on delinquency: A longitudinal comparison of labeling and deterrence theories." *J. Crim. L. & Criminology* 75 (1984): 1222-1245.

Thomas, Christopher A. "The uses and abuses of legitimacy in international law." *Oxford Journal of Legal Studies* 34, no. 4 (2014): 729-758.

Tidy, Joe. “Ukraine says it is fighting first ‘hybrid war.’” *BBC News*, March 04, 2022. https://www.bbc.com/news/technology-60622977.

Tischler, Mark. “China’s ‘Never Again’ Mentality.” *The Diplomat*, August 18, 2020. https://thediplomat.com/2020/08/chinas-never-again-mentality/.

T-Mobile. “T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack.” *T-Mobile*, August 27, 2021. https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation.

Tomz, Michael. "Domestic audience costs in international relations: An experimental approach." *International Organization* 61, no. 4 (2007): 821-840.

Torres, Walter J., and Raymond M. Bergner. "Humiliation: its nature and consequences." *Journal of the American Academy of Psychiatry and the Law Online* 38, no. 2 (2010): 195-204.

Tossini, J. Vitor. "The Five Eyes – The Intelligence Alliance of the Anglosphere." *UK Defence Journal*, April 14, 2020. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/.

Tucker, Eric, and Tami Abdollah. "Iranian hacker indictment part of US name-and-shame tactic." *AP News*, March 25, 2016. https://apnews.com/article/1db343da098540c1a31b13be032df263.

Tuma, Shawn E. "Yes, Case Law Says It Really Is A CFAA Violation To DDoS A Website." *Business Cyber Risk,* October 09, 2013. https://shawnetuma.com/2013/10/09/yes-case-law-says-it-really-is-a-cfaa-violation-to-ddos-a-website/.

U.S. Attorney's Office for the Central District of California. "Los Angeles Grand Jury Indicts Chinese National In Computer Hacking Scheme Allegedly Involving Theft Of Trade Secrets." *U.S. Department of Justice*, August 15, 2014. https://www.justice.gov/usao-cdca/pr/los-angeles-grand-jury-indicts-chinese-national-computer-hacking-scheme-allegedly.

U.S. Attorney's Office, Central District of California. "Russian Hacker Sentenced to Nearly 6 Years in Prison in Scheme that Caused $4.1 Million in Losses with Fraudulent Debit Cards." *U.S. Department of Justice,* July 27, 2018. https://www.justice.gov/usao-cdca/pr/russian-hacker-sentenced-nearly-6-years-prison-scheme-caused-41-million-losses.

U.S. Attorney's Office, District of Columbia. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." *U.S. Department of Justice,* August 27, 2020. https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two.

U.S. Attorney's Office, District of Massachusetts. "Two Alleged Hackers Charged with Defacing Websites Following Killing of Qasem Soleimani." *U.S. Department of Justice,* September 15, 2020. https://www.justice.gov/usao-ma/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani.

U.S. Attorney's Office, District of New Jersey. "Two Iranian Nationals Charged in Cyber Theft and Defacement Campaign Against Computer Systems in United States, Europe, and Middle East." *U.S. Department of Justice,* September 16, 2020. https://www.justice.gov/usao-nj/pr/two-iranian-nationals-charged-cyber-theft-and-defacement-campaign-against-computer.

U.S. Attorney's Office, Eastern District of Virginia. "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election." *U.S. Department of Justice,* September 17, 2020. https://www.justice.gov/usao-edva/pr/iranian-hackers-indicted-stealing-data-aerospace-and-satellite-tracking-companies.

U.S. Attorney's Office, Northern District of Georgia. "United States v. Dimitry Belorossov a/k/a Rainerfox." *U.S. Department of Justice,* November 25, 2015. https://www.justice.gov/usao-ndga/victim-witness-assistance/information-victims-large-cases/united-states-v-dimitry-belorossov-aka-rainerfox.

U.S. Attorney's Office, Southern District of New York. "Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO." *U.S. Department of Justice,* November 27, 2017. https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

U.S. Attorney's Office, Southern District of New York. "MANHATTAN U.S. ATTORNEY AND FBI ASSISTANT DIRECTOR-IN-CHARGE ANNOUNCE EXTRADITION OF RUSSIAN CITIZEN TO FACE CHARGES FOR INTERNATIONAL CYBERCRIMES." *U.S. Department of Justice,* January 17, 2012. https://www.justice.gov/archive/usao/nys/pressreleases/January12/zdoroveninvladimirandzdoroveninkirillindictment.html.

U.S. Attorney's Office, Southern District of New York. "Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court." *U.S. Department of Justice,* May 02, 2016. https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court.

U.S. Attorney's Office, Southern District of New York. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps." *U.S. Department of Justice,* March 23, 2018. https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.

U.S. Attorney's Office, Southern District of New York. "Russian Citizen Sentenced In Manhattan Federal Court To Three Years In Prison For Sophisticated International Cyber Crimes." *U.S. Department of Justice,* January 04, 2013. https://www.justice.gov/usao-sdny/pr/russian-citizen-sentenced-manhattan-federal-court-three-years-prison-sophisticated.

U.S. Attorney's Office, Southern District of New York. "U.S. Attorney Announces Charges Against Two Iranian Nationals For Cyber-Enabled Disinformation And Threat Campaign Designed To Interfere With The 2020 U.S. Presidential Election." *U.S. Department of Justice,* November 18, 2021. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-two-iranian-nationals-cyber-enabled.

U.S. Census Bureau. "QuickFacts." *U.S. Census Bureau*, 2021. https://www.census.gov/quickfacts/fact/table/US/PST045221.

U.S. Congress. "18 U.S. Code § 1030 - Fraud and related activity in connection with computers." *Cornell Law School Legal Information Institute,* October 20, 2020. https://www.law.cornell.edu/uscode/text/18/1030.

U.S. Congress. "18 U.S. Code § 371 - Conspiracy to commit offense or to defraud United States." *Cornell Law School Legal Information Institute,* September 13, 1994. https://www.law.cornell.edu/uscode/text/18/371.

U.S. Customs and Border Protection. "Customs Mutual Assistance Agreements (CMAA)." *U.S. Customs and Border Protection*, February 05, 2021. https://www.cbp.gov/border-security/international-initiatives/international-agreements/cmaa.

U.S. Department of Homeland Security. "U.S. Secret Service Arrests One of the World's Most Prolific Traffickers of Stolen Financial Information." *U.S. Department of Homeland Security*, July 07, 2014. https://www.dhs.gov/news/2014/07/07/us-secret-service-arrests-one-worlds-most-prolific-traffickers-stolen-financial.

U.S. Department of Justice. "205. When an Indictment is Required." *United States Department of Justice Archives: Criminal Resource Manual*, January 22, 2020. https://www.justice.gov/archives/jm/criminal-resource-manual-205-when-indictment-required.

U.S. Department of Justice. "9-15.000 - International Extradition And Related Matters." *Justice Manual*, April 2018. https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters.

U.S. Department of Justice: Office of Public Affairs. "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years." *U.S. Department of Justice,* October 30, 2018. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

U.S. Department of Justice: Office of Public Affairs. "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax." *U.S. Department of Justice,* February 10, 2020. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

U.S. Department of Justice: Office of Public Affairs. "Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act." *U.S. Department of Justice,* May 19, 2022. https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act.

U.S. Department of Justice: Office of Public Affairs. "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research." *U.S. Department of Justice*, July 19, 2021. https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

U.S. Department of Justice: Office of Public Affairs. "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election." *U.S. Department of Justice,* July 13, 2018. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

U.S. Department of Justice: Office of Public Affairs. "Man Pleads Guilty to Facilitating Computer Hacking of Vermont Company." *U.S. Department of Justice,* December 02, 2015. https://www.justice.gov/opa/pr/man-pleads-guilty-facilitating-computer-hacking-vermont-company.

U.S. Department of Justice: Office of Public Affairs. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." *U.S. Department of Justice,* March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

U.S. Department of Justice: Office of Public Affairs. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." *U.S. Department of Justice,* September 06, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

U.S. Department of Justice: Office of Public Affairs. "Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy." *U.S. Department of Justice,* November 30, 2017. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible.

U.S. Department of Justice: Office of Public Affairs. "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." *U.S. Department of Justice,* September 16, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

U.S. Department of Justice: Office of Public Affairs. "Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas." *U.S. Department of Justice,* March 09, 2022. https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas.

U.S. Department of Justice: Office of Public Affairs. "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe." *U.S. Department of Justice,* February 17, 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

U.S. Department of Justice: Office of Public Affairs. "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research." *U.S. Department of Justice,* July 21, 2020. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

U.S. Department of Justice: Office of Public Affairs. "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election." *U.S. Department of Justice,* November 18, 2021. https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.

U.S. Department of Justice: Office of Public Affairs. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." *U.S. Department of Justice,* May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

U.S. Department of Justice: Office of Public Affairs. "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage." *U.S. Department of Justice,* November 27, 2017. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

U.S. Department of Justice: Office of Public Affairs. "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." *U.S. Department of Justice,* March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

U.S. Department of Justice: Office of Public Affairs. "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya." *U.S. Department of Justice,* November 08, 2021. https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

U.S. Department of State, Office of Treaty Affairs. "Maldives (05-625) – Agreement Regarding Mutual Assistance Between Their Customs Administrations." *TREATIES AND OTHER INTERNATIONAL ACTS*, June 25, 2005. https://www.state.gov/wp-content/uploads/2019/02/05-625-Maldives-Customs.EnglishOCR.pdf.

U.S. Department of State. “Artem Valeryevich Ochichenko.” *Rewards for Justice,* April 2022. https://rewardsforjustice.net/rewards/artem-valeryevich-ochichenko/.

U.S. Department of the Treasury. “Cyber-related Designation; North Korea Designation Update.” *OFAC*, May 06, 2022. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506.

U.S. Department of the Treasury. “Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists.” *OFAC,* 2022. https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

U.S. Department of the Treasury. “Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses.” *OFAC*, November 28, 2018. https://home.treasury.gov/news/press-releases/sm556.

United Nations. “War Crimes.” *United Nations Office on Genocide Prevention and the Responsibility to Protect,* n.d. https://www.un.org/en/genocideprevention/war-crimes.shtml.

Vaas, Lisa. “100m T-Mobile Customer Records Purportedly Up for Sale.” *ThreatPost,* August 16, 2021. https://threatpost.com/t-mobile-investigates-100m-records/168689/.

Vaas, Lisa. “T-Mobile’s Security Is ‘Awful,’ Says Purported Thief.” *ThreatPost*, August 28, 2021. https://threatpost.com/t-mobile-security-awful-thief/169011/.

Vasquez, Maegan. “Russia issues sanctions against Biden and a long list of US officials and political figures.” *CNN,* March 15, 2022. https://www.cnn.com/2022/03/15/politics/biden-us-officials-russia-sanctions/index.html.

Verkhovna Rada of Ukraine. “Criminal Code of Ukraine.” *U.S. Department of Justice,* September 01, 2001. https://www.justice.gov/sites/default/files/eoir/legacy/2013/11/08/criminal_code_0.pdf.

Verkhovna Rada of Ukraine. “Criminal Procedure Code of Ukraine.” *Council of Europe,* 2015. https://rm.coe.int/16802f6016.

Viskupič, Filip. "Experimental evidence on prestige attribution in international relations." *The Social Science Journal* (2021): 1-14.

Viswanatha, Aruna, and Joseph Menn. “In cyberattacks such as Sony strike, Obama turns to 'name and shame'.” *Reuters*, January 14, 2015. https://www.reuters.com/article/uk-usa-cybersecurity/in-cyberattacks-such-as-sony-strike-obama-turns-to-name-and-shame-idUSKBN0KN2E520150114.

Waldrop, M. Mitchell. "How to hack the hackers: The human side of cybercrime." *Nature* 533, no. 7602 (2016).

Walker, Shaun. "Russia hits out at 'kidnapping' of MP's son by US secret service." *Guardian,* July 08, 2014. https://www.theguardian.com/world/2014/jul/08/russia-mps-son-seleznev-arrest-us-secret-service.

Wall Street Journal. "Mandiant: No Drop in Chinese Hacking Despite Talk." *Wall Street Journal*, April 24, 2013. https://www.wsj.com/articles/BL-CJB-17624.

Walsh, Emily. "T-Mobile customers are left feeling frustrated as hacker comes forward, calling the company's security 'awful'." *Business Insider*, August 28, 2021. https://www.businessinsider.com/t-mobile-customers-frustrated-hacker-says-security-is-awful-2021-8.

Ward, David A., and Charles R. Tittle. "Deterrence or labeling: The effects of informal sanctions." *Deviant Behavior* 14, no. 1 (1993): 43-64.

West, Mark D. "Losers: Recovering Lost Property in Japan and the United States." *Law & Society Review* 37, no. 2 (Jun. 2003): 369-424.

West, Robin. "Classical Criminology." *The Wiley-Blackwell Encyclopedia of Social Theory* (2017): 1-4.

White House: Office of the Press Secretary. "AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES OF AMERICA AND THE GOVERNMENT OF THE RUSSIAN FEDERATION ON COOPERATION AND MUTUAL ASSISTANCE IN CUSTOMS MATTERS." *National Archives: Clinton Presidential Materials Project*, September 28, 1994. https://clintonwhitehouse6.archives.gov/1994/09/1994-09-28-us-russian-agreement-on-customs-matters.html.

White House: Office of the Press Secretary. "FACT SHEET: President Xi Jinping's State Visit to the United States." *The White House: President Barack Obama*, September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.

Whitney, Lance. "The many sides of DarkSide, the group behind the Colonial Pipeline ransomware attack." *TechRepublic,* May 11, 2021. https://www.techrepublic.com/article/the-many-sides-of-darkside-the-group-behind-the-colonial-pipeline-ransomware-attack/.

Whittaker, Zack. "US offers bounty for Sandworm." *TechCrunch*, April 27, 2022. https://techcrunch.com/2022/04/27/state-sandworm-russian-hackers-ukraine/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACNQvI4b55qHffj2tHBQs-inYnIC7x88isX3tO6DdWUATvAIlc5LgtwWyELVTdiIIycE7Ov8i6hGIBJXHLgph85EjqL

Bm3Fm0V6qarI2Kx6gdig3uimS06dCZJtwRquYfjezlchiJSev1F87mKY06Pt8RTeV3-UN7rFyDyPP4gFw.

Williams, Kirk R., and Richard Hawkins. "Perceptual research on general deterrence: A critical review." *LAw & Soc'Y REv*. 20 (1986): 545.

Williams, Robert D. "America's Hopelessly Anemic Response to One of the Largest Personal-Data Breaches Ever." *Atlantic*, February 12, 2020. https://www.theatlantic.com/ideas/archive/2020/02/whats-behind-the-indictment-of-the-equifax-hackers/606466/.

Wilner, Alex S. "US cyber deterrence: Practice guiding theory." *Journal of Strategic Studies* 43, no. 2 (2020): 245-280.

Wirtz, James J. "How does nuclear deterrence differ from conventional deterrence?" *Strategic Studies Quarterly* 12, no. 4 (2018): 58-75.

Wittes, Benjamin. "James Lewis on the China Cyber Deal." *Lawfare,* October 05, 2015. https://www.lawfareblog.com/james-lewis-china-cyber-deal.

Wittes, Benjamin. "Maybe Those Chinese Cyber Espionage Indictments Weren't So Dumb." *Lawfare,* December 01, 2015. https://www.lawfareblog.com/maybe-those-chinese-cyber-espionage-indictments-werent-so-dumb.

Wolfrum, Rüdiger. "Legitimacy in International Law." *Oxford Public International Law,* March 2011. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1960.

Xi, Jinping. "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era." Transcript of speech delivered at 19th National Congress of the Communist Party of China, October 19, 2017. http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

Yannis, Alexandros. "The Concept of Suspended Sovereignty in International Law and Its Implications in International Politics." *European Journal of International Law* 13, no. 5 (2002): 1037-1052.

Zagare, Frank C. "Rationality and deterrence." *World Politics* 42, no. 2 (1990): 238-260.

Zagare, Frank C., and D. Marc Kilgour. "Deterrence theory and the spiral model revisited." *Journal of Theoretical Politics* 10, no. 1 (1998): 59-87.

Zegart, Amy. “Everybody spies in cyberspace.” *Atlantic*, December 30, 2020. https://www.theatlantic.com/ideas/archive/2020/12/everybody-spies-cyberspace-us-must-plan-accordingly/617522/.

Zetter, Kim. “Mastermind Behind Gozi Bank Malware Charged Along With Two Others.” *Wired,* January 23, 2013. https://www.wired.com/2013/01/mastermind-behind-gozi-charged/.

Zetter, Kim. “The Most Controversial Hacking Cases of the Past Decade.” *Wired*, October 26, 2015. https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/.