Title

Privatization, Technology, and the Transformation of Global Security: An Analysis of International Legal and Normative and Challenges

Author

Shandro, Angélina

Publication Date

2024-04-01

Privatization, Technology, and the Transformation of Global Security:

An Analysis of International Legal and Normative and Challenges

Angélina Shandro

Undergraduate Political Science Thesis

University of California, Los Angeles

1 April 2023

Abstract

Historically, the privilege of legitimately waging war was arrogated exclusively to states and their militaries. Yet in the 21st-century geopolitical and strategic environment, states have increasingly externalized the burdens of conflict to private actors operating across the military, security, cyber, and intelligence domains. In recognition of these developments, this inquiry evaluates the following research question: To what extent have multilateral initiatives effectively addressed the practical, legal and normative challenges presented by the increasing legitimacy and influence of private actors in contemporary conflicts? Part A of this inquiry contemplates the sources underpinning commercial security providers' authority and legitimacy, explores the structural conditions contributing to their increased use by governments, and considers how the interaction of privatization and technological development challenge traditional legal and normative principles. Through a comparative case study analysis, Part B evaluates the efficacy of the hard-law Draft Convention, the state-sponsored Montreux Document, the industry-sponsored International Code of Conduct, and the Wassenaar Arrangement export control regime in contributing to the articulation and implementation of new norms and laws regarding warfare's privatization. Several patterns are evident across these multilateral initiatives, regarding their tendency to generate participation and enforcement issues, to normalize and legitimate commercial security providers through legal discourse, to disproportionately empower some actors at the expense of others, and to struggle to balance idealistic norms within concrete political realities. This analysis not only illuminates international actors' attempts to understand and regulate warfare's privatization given the challenges that technologically advanced, privatized conflict poses to existing legal frameworks. It also concretely demonstrates how the terrain of international law remains entangled in the subjectivities of international politics. Academic engagement regarding this complex, unprecedented challenge to international security remains imperative for guiding future decision-making regarding the governance of warfare.

Table of Contents

Introduction

Historically, the privilege of legitimately waging war was arrogated exclusively to states and their militaries. Yet in the 21st-century's geopolitical and strategic environment characterized by rapid globalization and technological development, states have increasingly externalized the burdens of conflict to private actors. Unlike traditional soldiers engaged in overt, direct combat, these actors' capabilities span the realms of military, security, cyber and intelligence. They frequently operate transnationally and clandestinely, blurring the traditional spatio-temporal concept of the "battlefield", the distinction between "civilian" and "combatant", and ultimately the boundary between "war" and "peace". As the most brutal forms of intimidation are increasingly superseded by more subtle mechanisms of coercion, Clausewitz's 'fog of war' increases exponentially. These dynamics have challenged the viability of the laws and customs traditionally used to hold actors accountable, and guide principled responses within the international community. Rather than contemplating the specificities and theoretical application of international principles as they relate to commercial security providers, this research focuses on state and corporate practice to evaluate the nature, scope, and prospects of emerging laws and norms regarding the privatization of conflict. Academic engagement regarding this complex, unprecedented challenge to international security remains imperative for guiding future decision-making regarding the governance of warfare.

Literature Review

An overview of the extant literature situates this inquiry at the intersection of prior research regarding the privatization of warfare through military, security, cyber, and intelligence companies, and the challenges associated with their regulation under existing international legal frameworks. Part 1 of the literature review defines the concept of "hybrid warfare", and outlines scholars' prior efforts to identify the legal

and policy implications associated with these unprecedented tactics and mechanisms of contemporary conflict. The scope of inquiry is subsequently narrowed to consider private military and security companies (PMSCs), the actors enabling hybrid warfare. Following an analysis of the structural conditions underpinning the emergence of this "market for force" and a consideration of the ambiguities inherent in categorizing these actors, the discussion considers how contemporary private military and security companies have taken advantage of technological development to augment their cyber and intelligence capabilities. Evaluating the structural conditions for this new iteration of privatized security leads to a discussion of governments' role in actively creating and sustaining demand for commercial proxies when engaging in conflicts. After outlining the industry's development and its core features, Part 2 explores the applicability of several international norms and laws to private military and security companies. The evolution of the state monopoly on violence and the anti-mercenary norm are considered, in addition to laws regarding state responsibility for these actors. Finally, recognizing the chaotic legal and normative milieu in which privatized conflict occurs, Part 3 draws on insights from critical legal scholarship emphasizing the dynamic, subjective, and contestable nature of international laws and norms. These ideas are advanced as a foundation for the following analysis of contemporary multilateral efforts to define and regulate privatized warfare.

Part 1: The Privatization of Warfare

Hybrid Warfare

A substantial body of research highlights the inapplicability of traditional laws of conflict as new technologies facilitate hybrid warfare.[1] "Hybrid warfare" refers to the simultaneous combination of conventional military tactics with irregular, non-kinetic operations within the same battlespace, in order to

[1] Braden R. Allenby, "Are New Technologies Undermining the Laws of War?," *Bulletin of the Atomic Scientists* 70, no. 1 (2014), https://doi.org/10.1177/0096340213516741.

achieve strategic political objectives by creating exploitable ambiguity.[2] These unconventional methods span the criminal and cyber domains, and frequently limit the targeted entity's recourse to lawful responses.[3] Typically, actors employing hybrid warfare tactics seek to weaken and destabilize the enemy without perceived involvement, avoiding responsibility and retribution for their actions.[4] According to Al Aridi, the ambiguities and power asymmetries generated by hybrid warfare campaigns, "mainly through cyber operations and the employment of [non-state actors]… that operate covertly", introduce significant legal complexities.[5]

Most authors in this field conduct threat assessments concerning a single country's strategic objectives, and propose policy responses based primarily on domestic military doctrines rather than international law.[6] Nevertheless, some scholars have explored the legal dimensions of hybrid warfare-induced security and human rights dilemmas. Considerable methodological diversity exists within the extant scholarship, each with its own advantages and limitations. Several authors employ a legal-ethical perspective, substantiating theoretical insights with close readings of key statutes, and analyses of international organizations' responses.[7] Others invoke case studies to illustrate the exploitation of legal ambiguities resulting from emergent technological asymmetries.[8] Through a unique game-theoretic approach drawing

[2] Vladimir Rauta, "Towards a Typology of Non-state Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces," *Cambridge Review of International Affairs* 33, no. 6 (2019): 869, https://doi.org/10.1080/09557571.2019.1656600.
[3] Laura A. Dickinson, "Contractors and Hybrid Warfare: A Pluralist Approach to Reforming the Law of State Responsibility," in *States, Firms, and Their Legal Fictions*, ed. Melissa J. Durkee (Cambridge University Press, 2024), 78, https://doi.org/10.1017/9781009334709.005.
[4] Dennis Broeders et al., *Artificial Intelligence and International Conflict in Cyberspace* (New York, NY: Routledge, 2023), 56, https://doi.org/10.4324/9781003284093.
[5] Alaa Al Dakour Al Aridi, "The Problem of Hybrid Warfare in International Law" (PhD diss., Vilnius University, 2022), 13.
[6] Sean Monoghan, "Countering Hybrid Warfare So What for the Future Joint Force?," *PRISM* 8, no. 2 (2019), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf.
[7] Morten M. Fogt, "Legal Challenges or 'Gaps' by Countering Hybrid Warfare - Building Resilience in Jus Ante Bellum," *Southwestern Journal of International Law* 27, no. 1 (2021), https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf.
[8] Sascha-Dominik Bachmann and Håkan Gunneriusson, "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security," *Scientia Militaria: South African Journal of Military Studies* 43, no. 1 (2015), https://doi.org/10.5787/43-1-1110.

on defense economics, Balcaen, Bois and Buts capture this evolving security paradigm's theoretical nuances and complexities.[9] Although Balcaen et al. provide substantive policy advice based on the threats identified, they do not offer empirical observations to legitimize their model's practical utility. Even among analyses referencing international statutes and customs, acknowledgment of the law's politicization is often neglected.[10] These insights demonstrated that the extant literature regarding the relationship between hybrid warfare and law disproportionately focuses upon tactics employed in the socio-political, economic, and informational domains, at the expense of contemplating *by whom* these measures are enacted. Nevertheless, a related body of literature has identified private military and security companies as actors fundamentally supporting hybrid warfare operations. The following section outlines the structural factors underpinning private military and security companies' rise to prominence, and the transformation and expansion of their operations from conventional kinetic combat functions towards technologically-oriented services in the cyber and intelligence domains.

Private Military and Security Companies: Structural Conditions for Industry Emergence

For the purposes of this inquiry, private military and security companies (PMSCs) are defined under the Montreux Document as "private business entities that provide military and/or security services, irrespective of how they describe themselves… [including] armed guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel".[11]

---

[9] Pieter Balcaen, Cind Du Bois, and Caroline Buts, "A Game-theoretic Analysis of Hybrid Threats," *Defence and Peace Economics* 33, no. 1 (2021), https://doi.org/10.1080/10242694.2021.1875289.
[10] Aurel Sari, "Hybrid Warfare, Law, and the Fulda Gap," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, ed. Winston S. Williams and Christopher M. Ford (Oxford University Press, 2018), https://doi.org/10.1093/oso/9780190915360.003.0006.
[11] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Art. 9(a), August 2009, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf.

The literature regarding privatized force has comprehensively identified and examined several structural conditions contributing to the burgeoning industry for private violence, including the end of the Cold War, resulting changes in the supply and demand of security, and the transforming nature of warfare itself.[12] The Cold War's conclusion generated a security vacuum and a dramatic increase in domestic violence as the discipline previously exercised by global superpowers receded; the implosion of many weak states and resumption of border conflicts generated governance failures and a demand for private security firms.[13] Meanwhile, former Communist states, the United States (US), and the United Kingdom (UK) were downsizing their militaries and outsourcing security operations (partially motivated by defense budget-saving pressures), and the dismantling of South Africa's apartheid regime generated a pool of experienced personnel for hire.[14,15] The surplus of military labor was accompanied by a parallel flood of military equipment into the market at relatively low prices, increasing potential profitability.[16] These forces of supply and demand catalyzed the development of the global market for force, generating organized private entities that could be better trained and equipped than their State counterparts.[17]

Note that the Montreux Document definition does not encompass combat provider companies, whereas the United Nations Convention on Mercenaries employs a broader definition encompassing all contractors supporting armed forces (regardless of what service they provide). However, both definitions specifically omit combat activities. To avoid conceptual confusion, this paper employs the Montreux Document definition.

[12] Berenike Prem, "Who Am I? The Blurring of the Private Military and Security Company (PMSC) Category," *Security Privatization* (2017): 52, https://doi.org/10.1007/978-3-319-63010-6_3.

[13] Hin-Yan Liu, *Law's Impunity: Responsibility and the Modern Private Military Company* (Oxford, United Kingdom: Hart Publishing, 2017), 96.

[14] A.C Cutler, "The Legitimacy of Private Transnational Governance: Experts and the Transnational Market for Force," *Socio-Economic Review* 8, no. 1 (2009), https://doi.org/10.1093/ser/mwp027.

[15] The culture of outsourcing and neoliberal ideologies endorsed by the Reagan-Thatcher administrations underpinned these trends in the United Kingdom and the United States. See Liu, *Law's Impunity,* 96.

[16] of International Law: The Life Cycle of Emerging Norms on the Use and Regulation of Private Military and Security Companies," *Griffith Law Review* 26, no. 1 (2017): 94, https://doi.org/10.1080/10383441.2017.1339773.

[17] Liu, *Law's Impunity*, 96.

Ambiguities Regarding Classification of Private Military and Security Companies

The conceptual confusion surrounding the categorization of various actors in the industry for privatized force is well established in the extant literature. Implicit in these categorizations is the notion that a PMSC occupies a static position along a continuum of force, with providing lethal force on the frontlines at one end of the spectrum, and undertaking logistical and administrative functions at the other.[18] However, dividing PMSCs into ideal-typical companies based on their relationship to the battlespace and the extent of force employed in performing their services neglects the fact that many PMSC's activities blur the boundary between lethal/non-lethal, combat/non-combat, and offensive/defensive activities.[19,20] In fact, a single company's capabilities can span myriad functions, from combat and armed security services, to logistics and technical support, to intelligence and surveillance. Other taxonomies, predicated on the distinction between military provider, military consultant, and military support firms are similarly challenged by the low level of specialization characterizing most companies, the increasingly technological nature of warfare, and the complexities of asymmetric conflicts and operations outside traditional, overt conflict.[21] For example, the outsourcing of intelligence and military weaponry operational support has endowed unarmed contractors —working far from the frontline and carrying out activities ostensibly classified as logistical support— with significant responsibility in the deployment of lethal force. Development of a concrete typology to categorize such multifaceted entities remains elusive, undermining the international community's understanding of their functioning, and ability to effectively regulate them.

[18] P.W Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, 2nd ed. (Ithaca, N.Y.: Cornell University Press, 2008).
[19] Prem, "Who Am I," 52.
[20] Rauta, "Towards a Typology".
[21] Eugenio Cusumano, "Policy Prospects for Regulating Private Military and Security Companies," *War by Contract*, January 1, 2011, 15, https://doi.org/10.1093/acprof:oso/9780199604555.003.0002.

Private Military and Security Companies and Technological Development: A New Iteration of Privatized Security

Historically, the most technologically advanced governments dominated the cyber domain, and intelligence functions were restricted to the most trusted institutions of the state. However, an assortment of private firms now offers their services in an expanding industry for technical vulnerabilities (with numerous companies formed by intelligence analysis and operators rendered superfluous since the end of the Cold War).[22] An intriguing subsector of the privatized warfare operations industry, private intelligence and spyware companies provide a variety of defensive and offensive services: the former includes protecting government networks against malware, identifying vulnerabilities, or increasing computer systems' resilience, whereas the latter involves gaining access to an adversary's computer system and taking advantage of vulnerabilities within that network.[23] In contrast to the kinetic combat, security, and support services characteristic of traditional PMSCs, intelligence and cyber-oriented PMSCs operate in the digital realm, creating and deploying cyber-surveillance technologies (CSTs). CSTs refer to "devices, software and skills used by intelligence and law enforcement agencies, as well as network operators operating to secretly monitor, exploit, and analyze data stored, processed, and transferred over ICT".[24]

These entities' powerful position vis-à-vis states has been reinforced by the interplay of several conditions. Firstly, computer networks in cyberspace are predominantly owned and operated by private providers. As cyberspace and information technologies have become increasingly intrusive for societies, governments are increasingly dependent on private firms to provide them with technical expertise and

[22] Singer, *Corporate Warriors*, 99.
[23] Patrick Burkart and Tom McCourt, "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software," *Popular Communication*15, no. 1 (2017): 39, https://doi.org/10.1080/15405702.2016.1269910.
[24] Atul Alexander and Tushar Krishna, "Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism," *Laws* 11, no. 6 (2022): 9, https://doi.org/10.3390/laws11060085

operational capacities.[25] The widespread adoption of mobile technology has rendered every cellphone and computer an information-rich target a government might find useful for tracking perceived threats. However, technologies generally employ end-to-end encryption to protect sensitive communications, rendering it challenging for law enforcement agencies to access information via traditional wiretaps. Cyber-intelligence companies have developed powerful workarounds: instead of targeting encrypted data in transit, they offer uninhibited access to the mobile device itself.[26] Secondly, the private sector occupies a position as the primary innovator of revolutionary technologies in cyberspace, and there exists limited reliable knowledge regarding the dangers and vulnerabilities of this novel domain of warfare. This dynamic has rendered state actors increasingly dependent on private contractors to secure critical networks, exploit the communications of foreign adversaries, and provide foreign intelligence to domestic militaries.[27] Because data generation on malware and cyber incidents is costly and complex, the available information is largely based on private companies' reports; the authors have an incentive to inflate these threats and encourage government actors to seek their services. Finally, the lack of success in foreign interventions in Iraq, Libya and Afghanistan has undermined demand for commercial actors in supporting large-scale multilateral commercial operations. [28] Instead, national security strategies are evolving toward remote or 'hybrid' warfare tactics. Given the mutually reinforcing nature of these three conditions, PMSCs not only operate computer networks and develop the key technological innovations, but define the nature of the policy challenge itself. In contrast to the industry traditional PMSCs, a private market for cybersecurity services and tools already existed by the time governments began contemplating cyberspaces as a domain for non-kinetic operations.[29] Contemporary digitalization has brought about the

[25] Moritz Weiss, "The Rise of Cybersecurity Warriors?," *Small Wars and Insurgencies*33, nos. 1-2 (2021): 277, https://doi.org/10.1080/09592318.2021.1976574.
[26] George T. Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," *Harvard Human Rights Journal* 36, no. 2 (2023): 199, https://journals.law.harvard.edu/hrj/wp-content/uploads/sites/83/2023/06/HLH105_crop.pdf.
[27] Weiss, "The Rise," 285.
[28] Fogt, "Legal Challenges," 48.
[29] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom: Cambridge University Press, 2018), 71.

rise of a new, increasingly powerful group of private companies that shape public policy for the sake of securing cyberspace.

Government Demand for Private Security- and Intelligence-Oriented PMSCs

Similarly to the demand for traditional PMSCs, governments have played a crucial role in the development of a market for software exploits used by PMSCs operating in the digital domain. Cybersecurity professionals have responded to demand signals from leaders seeking to stay ahead of their adversaries by pooling their talent through secretive firms, which essentially operate as government contractors for cyberweapons and spyware. The companies scan software for vulnerabilities, develop codes to exploit them, and sell or license the hacking tools to governments. The commodity chain for custom-configured spyware spans international labor and currency markets and free-trade regimes, yet because spyware production is complex and fraught with uncertainties, vendors frequently use a subscriptive business model.[30] Crucial to understanding the spyware industry is understanding the concept of zero-day vulnerabilities, referring to previously unknown software that expose the program to external manipulation.[31] These vulnerabilities create access to external networks and therefore undermine confidentiality and the integrity of information. The exchange value of zero-day exploits, based on their labor-intensive production and scarcity, is further enhanced by secrecy.[32] Zero-days are differentiated from other computer vulnerabilities —and are valuable— because they are unknown to the software's developers and users.[33] Some companies develop and sell weaponized vulnerabilities (zero-day exploits) containing new software code which takes advantage of a zero-day vulnerability. The value of secrecy complicates efforts to control the zero-day trade because it contributes to market opacity and a lack of

[30] Mailyn Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis," *I/S: A Journal of Law and Policy for the Information Society* 11, no. 2 (2015): 417, https://ssrn.com/abstract=2706199.
[30] Fidler, "Regulating the Zero-Day," 416.
[31] Asaf Lubin, *Selling Surveillance*, research report no. 495, 9, 2023, https://ssrn.com/abstract=4323985.
[32] Burkart and McCourt, "The International Political Economy", 44.
[33] Fidler, "Regulating the Zero-Day," 408.

transparency regarding buyer and seller behavior. The "grey market" as conceptualized by Fidler refers to "trade between vulnerability sellers and government agencies or other non-criminal clients"; it operates on a global scale, with British, Russian, Indian, Israeli, Brazilian, and Middle Eastern intelligence services identified as purchasers.[34,35] The negative security implications, lucrative nature, and global scope of zero-day trade have catalyzed widespread regulatory debate in the international legal realm. Government participation encourages grey market expansion, with potentially harmful ramifications for international cybersecurity.

The parameters of a multibillion-dollar industry of "digital mercenaries" has revealed itself, comprising firms-for-hire that sell cyber-armaments including "zero day" exploits, and coordinate targeted attacks on governments, corporations, and individuals.[36] Dozens of firms compete for clients, with industry leaders including Gamma Group, Hacking Team, and NSO Group. Intelligence and law enforcement agencies in at least 65 countries have purchased off-the-shelf services for surveillance purposes both internationally and domestically.[37] One must recognize that authoritarian regimes are not exclusively responsible for the dissemination and employment of spyware: frequently, these technologies originate from European and North American companies and are transferred worldwide through commercial relationships. For instance, The Surveillance Industry Index documents 526 companies in detail, noting that these entities are most likely to be headquartered and have offices in the US, the UK, France, Germany, Israel, and Italy.[38] Although ostensibly stateless, these companies have taken advantage of de facto state support, and the current uncertainty surrounding export control regimes designed for earlier eras of conflict. For

[34] Fidler, "Regulating the Zero-Day," 416.
[35] Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *The New York Times* (New York, NY), July 13, 2013, https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.
[36] David Kushner, "Fear This Man," *Foreign Policy*, April 26, 2016, https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/.
[37] Steven Feldstein, Governments are Using Spyware on Citizens Can They Be Stopped? 2021
[38] Heejin Kim, "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue," *International and Comparative Law Quarterly* 70, no. 2 (2021): 385, 386, https://doi.org/10.1017/s0020589321000105.

instance, the British government has prioritized cybersecurity exports since 2014, noting that they account for "30 percent of current UK security exports", and Israel's cybersecurity industry has "attracted a near four-fold increase in venture capital investment since 2010 [amid] a growing overseas market for cybersecurity".[39] These examples demonstrate how governments have actively created and sustained demand for the PMSC industry.

Part 2: Private Military and Security Companies Under Existing International Law

One critical perspective regarding PMSCs is the concern that these entities operate in a "legal vacuum" or a "grey zone" by circumventing the requirements imposed by the legal definition of mercenary, and by operating transnationally in situations below the "threshold" of armed conflict— such that international humanitarian law (IHL) does not specifically regulate PMSCSs.[40] This conceptualization is perhaps erroneous: emerging norms on PMSCs are not entirely new, but rather, constitute inchoate transformations of existing norms, particularly the anti-mercenary norm and the norm regarding the state monopoly on violence. These two norms are discussed below.

The State Monopoly on Violence

The Weberian understanding of a state monopoly over the legitimate use of violence (SMOV) has historically served as a cornerstone for international relations scholars' conceptualization of a state. For the purposes of this inquiry, the SMOV is defined as "the generalized expectation that sovereign governments or rulers should be the only actors who may legitimately use collective armed force", and

[39] Maurer, *Cyber Mercenaries*, 37.
[40] Sorensen, "The Politics," 99.

that citizens hold the exclusive right to wield force as members of national armies.[41] This concept is linked to the principle of "legitimate authority" inherent in *jus ad bellum,* stipulating that only the nation-state, as the authority providing public security, has the right to wage war. Emerging literature regarding the outsourcing of violence identifies how private actors complexify this traditional understanding of state authority. Mary Kaldor identifies this trend as one of the core features of contemporary forms of conflict— a perspective corroborated by Herfried Munkler in describing "new wars".[42,43] However, both scholars disproportionately focus on the phenomenon of bottom-up privatization, involving non-state actors arming themselves to provide for their own security in the context of civil warfare and state failure. Whereas this form of privatization fundamentally challenges the SMOV, top-down privatization, referring to governments outsourcing military and security tasks to commercial organizations, requires a more nuanced analysis.[44] Herbert Wulf distinguishes between top-down and bottom-up privatization, believing that both forms "undermine and fundamentally challenge the legitimate monopoly of force".[45] Yet in defining the SMOV, Weber clarifies that violence may be delegated: the "monopoly" on violence is conceptualized as exclusive power to authorize and legitimize the use of violence, rather than complete ownership over the actual means of violence.[46] It follows that the deliberate privatization of military and security functions does not necessarily erode the SMOV, but rather, as aptly argued by Avant, presents new tradeoffs to states.[47] These tradeoffs are examined in Part A of the Analysis section, with reference to the specific activities of PMSCs and governments.

---

[41] Elke Krahmann, "The United States, PMSCs and the State Monopoly on Violence: Leading the Way towards Norm Change," *Security Dialogue* 44, no. 1 (2013): 58, https://doi.org/10.1177/0967010612470292.
[42] Herfried Münkler, *The New Wars* (Cambridge, UK: Polity, 2005).
[43] Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era*, 2nd ed. (Cambridge: Polity, 2010).
[44] Eugenio Cusumano, *Mobilization Constraints and Military Privatization* (Springer International Publishing, 2023), 33, https://doi.org/10.1007/978-3-031-16423-1.
[45] Cusumano, *Mobilization Constraints*, 33.
[46] Max Weber, Hans Gerth, and C. Wright Mills, *Politics as a Vocation* (Hassell Street Press, 2021), 34.
[47] Deborah Avant, "The Privatization of Security and Change in the Control of Force," *International Studies Perspectives* 5, no. 2 (2004): 146, https://doi.org/10.1111/j.1528-3577.2004.00165.x.

The Anti-Mercenary Norm

Despite offering a logical starting point for a discussion of private military companies, the United Nations definition of "mercenary" has been rendered increasingly obsolete by the changing nature of warfare following the end of the Cold War. The anti-mercenary norm as it developed through the late 20th century is generally described as possessing two elements: mercenaries are foreign or external to the conflict in which they fight, and are motivated to fight primarily by financial gain.[48] This norm was institutionalized in international law in a variety of forms, including UN General Assembly and Security Council resolutions condemning the impact of mercenary activities on self-determination, the International Convention Against the Recruitment, Use, Financing, and Training of Mercenaries, and Article 47 of Additional Protocol I. Although the legal language describing what mercenaryism is and is not remains relatively clear, the early 21st century's iteration of private military actors deployed and supervised by corporations has complicated this legal definition. The broader trend of widespread outsourced security has redefined the international system's norms and laws, normalizing what would have been considered a deviation from international customs only a decade prior.

Increasing consensus exists within the scholarly literature that PMSCs and their employees cannot be designated as mercenaries on either formal or substantial grounds.[49] Despite sharing some similarities, PMSCs represent a new phenomenon unique from traditional mercenary ventures characterized by unstructured, clandestine forms of organization. The primary difference lies in PMSCs nature as legal entities based on permanent corporate structures with public recruitment patterns.[50] No longer operating underground or in an irregular manner, PMSCs are often established as registered business operations, hierarchically organized, and operate according to regularized procedures within a competitive,

[48] Sorensen, "The Politics".
[49] Eugenio Cusumano, "Policy Prospects for Regulating Private Military and Security Companies," *War by Contract*, January 1, 2011, https://doi.org/10.1093/acprof:oso/9780199604555.003.0002.
[50] Cusumano, *Mobilization Constraints*, 17.

transnational marketplace.[51] According to Singer, this dynamic has generated an entirely new level of legitimacy and connections for private military firms.[52] Some scholars, including Cusumano, assert that because they are corporate personalities with an established market existence, PMSCs ought to be subjected to a broader set of both legal and normative constraints.[53] Others, notably Swed and Burland, contend that because this new category of military actor is not designated as a mercenary, yet remains unrecognized as a soldier, a legal lacuna has emerged: PMSCs' rise constitutes a development in warfare that has outpaced the development of corresponding international legal categories, elucidating consequential gaps in regulation and accountability.[54]

Beyond the international norms described above, prior scholars have also considered established IHL and international human rights law (IHRL) principles regarding state responsibility and effective control, as they relate to commercial security providers. One must acknowledge that because IHL's invocation necessitates a protracted armed conflict between states, it is often of limited applicability in the context of PMSC activities. This occurs for two reasons. Firstly, given a hired PMSC's ability to obscure a state actor's involvement in a conflict, an otherwise "international" conflict may be seemingly transformed into a conflict fought between irregular forces or factions within a state. As a result, the conflict would be legally categorized as a non-international armed conflict, limiting a targeted states' opportunities for lawful recourse under IHL.[55] Secondly, as PMSCs expand their capabilities outside traditional combat functions to encompass services in the cybersecurity and intelligence realms (as previously discussed), their activities become increasingly unlikely to cross the threshold of "armed force" denoting an armed conflict. As a substantive example, cyber operations have become increasingly consequential for states as

[51] Cutler, "The Legitimacy", 161.
[52] Singer, *Corporate Warriors*.
[53] Cusumano, "Policy Prospects," 15.
[54] Ori Swed and Daniel Burland, "Outsourcing War and Security," in *Oxford Research Encyclopedia of Politics* (Oxford University Press, 2020), 9 https://doi.org/10.1093/acrefore/9780190228637.013.1925.
[55] Kristine A. Huskey, "Accountability for Private Military and Security Contractors in the International Legal Regime," *Criminal Justice Ethics* 31, no. 3 (2012): 2016, https://doi.org/10.1080/0731129x.2012.737169.

they can facilitate a range of long-term disruptive effects, yet states have no recourse to the legal justification for "self-defense" when cyber operations' effects have not crossed the threshold of an armed attack.[56] Ultimately, the distinction between situations of armed conflict (*jus in bello*) and situations prior to it (*jus ad bellum*) central to international law is complexified when military and security functions are outsourced to private actors.

Given the potentially limited relevance of IHL in the context of PMSCs, scholars have analyzed additional legal principles under IHRL in the context of PMSC activities. Firstly, because employing PMSCs instead of acting directly enables states to deny their involvement and potentially evade international legal obligations, it is critical to examine the law of state responsibility in the context of privatized conflict. This body of law is most comprehensively articulated within the ILC's Draft Articles of State Responsibility, drawn from the decisions of international tribunals. However, two relevant provisions, Articles 4 and 5, require such formal, direct links to the state that PMSCs and PCICs would likely not fall within their purview. For instance, Article 4(2) provides that a state is responsible for its "organs", including "any person or entity… [possessing] that status in accordance with the internal law of the state".[57] Absent a formal legal relationship between the PMSC and the state under domestic law defining that entity as a state organ (more than a merely contractual relationship for services), a state incurs responsibility for the PMSC only under "exceptional" circumstances, requiring the "complete… dependence" of the PMSC on the state.[58] Article 5 assumes a similarly formalist approach, providing that the conduct of "a person or entity which is not an organ of the state under Article 4 but which is empowered by the law of that state to exercise elements of… governmental authority shall be considered an actor of the state".[59] Whereas a state might be responsible for entities such as PMSCs that act

[56] Tim Maurer and Wyatt Hoffmann, *The Privatisation of Security and the Market for Cyber Tools and Services*, 9, 2019, https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf.
[57] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Art. 2(4), 2001, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[58] Dickinson, "Contractors and Hybrid," 79.
[59] International Law Commission, *Draft Articles*, Art. 5.

functionally with some element of governmental authority, the phrase "empowered by the law of that state" demands a formal legal relationship between the corporation and the government. Alternatively, Article 8 provides that the "conduct of a person or group of person shall be considered an act of a State under international law if… [they are] acting on the instructions of, or under the direction or control of, the State in carrying out that conduct".[60] Rather than resting on formal legal ties as in articles 4 and 5, this standard permits a functional approach contingent on the entity's actual behavior in relation to the state.[61] However, the threshold for establishing responsibility under Article 8 remains quite high: states can exploit this legal boundary by engaging with PMSCs in a manner that falls below the degree of "control" that would establish state responsibility.

The "effective control" test, endorsed by the International Law Commission in its Draft Articles on institutional responsibility, has garnered international acceptance as the method of attribution to international organizations and states. Developed by the International Court of Justice (ICJ) during the *Nicaragua* case, this standard of implies that a surrogate's action could be attributed to a patron only when the patron possessed effective control over the surrogate's activities, and could exercise sufficient pressure to direct their action.[62] This reading of control as "effective control" establishes a very high threshold for state responsibility that would allow states, at least legally, to evade any responsibility for PMSC misconduct.[63] Under international law, the "effective control" threshold does not capture the most salient practical consequences of proxy-state relationships— such as when a state either deliberately ignores a corporation's action, or creates so many degrees of separation that it cannot be legally held responsible (despite its clear involvement).[64] The less demanding "overall control" test was established by

[60] International Law Commission, *Draft Articles*, Art. 8.
[61] Dickinson, "Contractors and Hybrid," 80.
[62] The ICJ *Nicaragua* case considered whether the conduct of Nicaraguan contras as US surrogates was attributable to the United States.
[63] Krieg and Rickli, *Surrogate Warfare*, 158.
[64] Maurer, *Cyber Mercenaries*, 125.

the International Criminal Tribunal for The Former Yugoslavia (ICTY) in *Tadić.*[65] In this context, the Court rejected the stringent test established in *Nicaragua* and concluded that the state need only exercise "overall control" of the non-state actor to trigger responsibility.[66] If the ICTY's "overall control" standard is sufficient, contracting States would more frequently be responsible for conduct incidental to the execution of the contract by PMSCs. Although the "overall control" standard arguably provides a more effective test to attribute PMSCs' conduct to states, it, remains more contested within international law than the "effective control" standard.

This section demonstrated that the legal threshold for evading responsibility remains quite high, as demonstrated by Articles 4, 5 and 8 of the Draft Articles of State Responsibility. States have taken advantage of this boundary by engaging with PMSCs in a manner that does not constitute the degree of "control" denoting state responsibility. The ambiguous, contested nature of the meaning of "control", manifest as the stringent "effective control" test and less demanding "overall control" test further enables states to avoid legal attribution for PMSC operations under Article 8. In this regard, PMSCs offer a convenient mechanism for states wishing to engage in hybrid warfare; even if the contractors' presence is identified, it is difficult to demonstrate the necessary links to prove state responsibility.

Because the threats imposed through mechanisms of hybrid warfare in contemporary conflicts often seek to exploit gray areas and fault lines in existing laws, law and legal consideration are at the heart of hybrid warfare.[67] The preceding insights demonstrate PMSCs do not operate in a legal vacuum, but rather, in an extremely chaotic legal and normative environment characterized by diverse standards that were not intended to regulate contemporary manifestations of privatized warfare. By outsourcing military and security functions through the hiring of private contractors, states can frequently evade responsibility as a

[65] In *Tadić*, the court was assessing whether the Federal Republic of Yugoslavia maintained sufficient control over military forces operating in Bosnia to be considered a party to the armed conflict.
[66] Dickinson, "Contractors and Hybrid," 80.
[67] Sari, "Hybrid Warfare".

matter of international law, even when these actors commit atrocities or contravene other substantive international rules.[68]

Part 3: Critical Perspectives of International Laws and Norms

From a theoretical perspective, there exist significant limitations in applying traditional legal frameworks to PMSC activities. In particular, a rigid, positivist understanding of international law holds less utility in making sense of evolving, increasingly contested standards of appropriateness. It is therefore crucial to examine the practices and processes underlying states' and companies' efforts to articulate and implement new laws and norms. This research draws on critical legal scholarship as a foundation for understanding and articulating the legal and normative tensions introduced by warfare's privatization.

International Law as Subjective, Dynamic, and Continuously Evolving

Law is an especially powerful discourse because of its claim to 'depoliticize' issues under a claim to truth, rationality, and objectivity.[69] It fixes and freezes certain meanings —developed in particular circumstances and contexts— which become authoritative reference points until the law is amended or repealed. However, this ostensible 'neutrality' merely disguises the extent to which law is deeply implicated in conceptualizing and understanding the socio-political world in certain ways rather than others. Legal concepts such as "mercenaries", "criminals", "human rights", and "dual-use technologies" represent the construction or reinforcement of particular social categories and relationships, including the justification of the status quo and the legitimization of certain policies.[70] Because states are both subjects and creators of international law, international law constitutes a mechanism through which political power

[68] Dickinson, "Contractors and Hybrid".
[69] Berenike Prem, "The Regulation of Private Military and Security Companies: Analyzing Power in Multi-stakeholder Initiatives," *Contemporary Security Policy* 42, no. 3 (2021): 350, https://doi.org/10.1080/13523260.2021.1897225.
[70] Prem, "The Regulation," 350.

is employed, critiqued, justified, and restricted.[71] In this manner, laws ostensibly created to "constrain" state behavior regarding the use of force can equally "empower" these actors, essentially instructing them how to justify their behaviors in a manner that does not contravene the law.[72] Finally, a critical perspective recognizes international law's inherent fragmentation: there is no single legislative will behind international law, and treaties and customs emerge from perpetual bargaining and negotiating among actors with conflicting underlying motives and objectives.[73] According to Koskenniemi, this process of contestation is underpinned by a tension between the requirements of normativity and concreteness. Concreteness concerns "the need to verify the law's content, not by reference to some political principles but… to the concrete behavior, will, and interest of States". Normativity refers to "the capacity of the law to be opposable to State policy".[74] Part B of the analysis draws on Koskenniemi's ideas regarding normativity and concreteness as a point of departure for examining the politics of international law in relation to emerging norms on PMSCs.

The Significance of International Norms

Normative order is linked to international law, but is also shaped outside law and goes beyond it. Norms refer to "standard[s] of appropriate behavior for actors with a given identity". In their extensively cited "norm life cycle" model, Martha Finnemore and Kathryn Sikkink argue that norms emerge in the international system through the endeavors of norm entrepreneurs in persuading state actors to adopt new

[71] Bibi van den Berg and Dennis Broeders, eds., *Governing Cyberspace: Behavior, Power, and Diplomacy*, 89, 2020, https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf
[72] Ian Hurd, "The International Rule of Law and the Domestic Analogy," *Global Constitutionalism* 4, no. 3 (2015): 63-65, https://doi.org/10.1017/s2045381715000131.
[73] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 895, https://doi.org/10.1162/002081898550789.
[73] Kim Sorensen, "The Politics of International Law: The Life Cycle of Emerging Norms on the Use and Regulation of Private Military and Security Companies," *Griffith Law Review* 26, no. 1 (2017): 92, https://doi.org/10.1080/10383441.2017.1339773.
[74] Martti Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge: Cambridge University Press, 2015), 58.

norms.[75] They identify a three-stage process through which norms become legitimate. In the first phase, norm entrepreneurs with sufficient organizational platforms persuade enough actors to agree with the norm to reach a "tipping point". Norm entrepreneurs can be motivated by a range of interests, such as effective global governance, consolidation of geopolitical influence, and profit maximization.[76] Subsequently, the norm entrepreneurs (referring in this case to states and PMSCs) collaborate with other actors (such as international organizations and NGOs) to legitimize the norm, in a process of socialization and institutionalization.[77] Finally, the norms become embedded in society through the phase of internalization, which entails legal, professional, and bureaucratic processes causing norm adherence to become largely automatic.[78] Because norms simultaneously influence state actors' behavior and are shaped and transformed by this behavior, norms are in a perpetual process of contestation, and re-definition.[79] For the purposes of Part B of this inquiry, the model of norm change offers a heuristic point of departure for explaining the development and crystallization of international norms and laws regarding PMSCs.

Gap in Literature and Research Question

Gap in Existing Literature

In examining the rise of hybrid warfare, several scholars have evaluated the structural and functional conditions facilitating the increasing privatization of security functions. Other authors have illuminated the consequences of the ever-increasing range of cybersecurity and spyware, hacking, and intelligence capabilities sold by private actors to governments. However, despite extensively analyzing these two

[75] Finnemore and Sikkink, "International Norm," 895.
[76] Sorensen, "The Politics," 92.
[77] Ingvild Bode and Hendrik Huelss, *Autonomous Weapons Systems and International Norms* (Montreal, QC: McGill-Queen's University Press, 2022), 137.
[78] Finnemore and Sikkink, "International Norm," 898.
[79] Elke Krahmann, "The United States, PMSCs."

important aspects of hybrid warfare —the privatization of security functions and technological development— are frequently analyzed in isolation. The present inquiry addresses this gap by contemplating the industry's evolution from offering kinetic, tangible services concerned with combat and support functions, towards additional intangible capabilities in the cyberspace. This allows for an exploration regarding the extent to which technological development may compound the challenges posed to existing norms and laws by traditional, combat-oriented PMSCs.

Moreover, discussions regarding PMSCs are often restricted to threat analyses or policy advice but do not contemplate the legal challenges posed by their activities. A separate body of literature has extensively analyzed customary and codified international law as it may relate to, or implicate, PMSCs; however, these analyses are theoretical in nature and remain somewhat divorced from the practical realities of PMSC-state relations. Rather than offering an exegesis of existing norms and rules, this research focuses on multi-stakeholder initiatives specifically designed to address PMSC's behavior. Examining emerging norms and laws regarding PMSCs concentrates on elucidating their embeddedness within institutions and interactions, highlighting the context-bound character of social actualities. Finally, whereas prior discussions of hybrid warfare often foreground the inapplicability of existing laws and actors' efforts to exploit them, this analysis will explore the productive dimensions of law and custom formation.

Research Question

These observations have generated the following research question:

To what extent have multilateral initiatives effectively addressed the practical, legal and normative challenges presented by the increasing legitimacy and influence of private actors in contemporary conflicts?

For the purposes of this inquiry, "effectiveness" indicates the degree to which new treaty laws, principles, and policy norms succeed in emerging and being institutionalized through the "norm life cycle" process described in the literature review. "Legitimacy" refers to the perception that the externalization of security functions to private actors is "desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs and definitions.[80] "Influence" concerns these actors' ability to meaningfully affect the nature and outcomes of contemporary international conflicts. Lastly, "private actors" in this context denotes companies offering both kinetic and non-kinetic services across the military, security, cyber and intelligence realms (referred to as PMSCs throughout the analysis).

Argument

To comprehensively evaluate the research question, this inquiry is divided into Part A (which contemplates PMSCs sources of legitimacy, and the challenges they present to international laws and norms), and Part B (which analyzes the international community's efforts to confront these challenges). Part A argues that PMSCs derive their legitimacy and authority based on their status as security and risk experts, their efficiency as market actors, and their ability to distance themselves from the controversial "mercenary" label by offering diverse services. These actors have introduced new complexities within international conflict environments: in particular, the plausible deniability with which PMSCs provide governments generates challenges internationally in attributing state responsibility, and domestically in ensuring transparency in security matters between governments and their own citizens. Technological developments in cyberspace and intelligence capabilities, insofar as they have been adopted by PMSCs, have exacerbated these existing issues by allowing private actors to operate cross-jurisdictionally and clandestinely. PMSCs' increasing international relevance, in conjunction with governments' demand for their services, have encouraged the evolution of norms regarding the traditional prohibition on

[80] Ori Swed and Thomas Crosbie, eds., *The Sociology of Privatized Security* (Springer International Publishing, 2019), 68,69, https://doi.org/10.1007/978-3-319-98222-9.

outsourcing functions inherent to the state. Next, Part B compares various multilateral fora (a hard law mechanism, industry- and state-orchestrated soft law initiatives, and an export control regime) designed to address the legal and normative issues identified in Part A. Part B contends that these initiatives reproduce many of the challenges they seek to address. This occurs due to their tendency generate participation and enforcement issues, to normalize and legitimate PMSCs through legal discourse, and disproportionately empower some actors at the expense of others, as they struggle to balance idealistic norms within concrete political realities.

Methodology

The qualitative case study approach constitutes a promising method to pursue for several reasons. Firstly, the study of cyber and intelligence proxies is still in its infancy, characterized by data that is very limited, often classified or proprietary, and sometimes outright contradictory. Given this information-ambiguous environment, a comparative case-study approach "gives the researcher an opportunity to fact-check, to consult multiple sources… and to overcome whatever biases may affect the secondary literature".[81] Other scholars conducting similar inquiries regarding different countries' usage of PMSCs,[82,83] the activities of particular companies,[84] and the laws applicable to PMSCs.[85]

Moreover, the research's protean nature lends itself to a more inductive approach, where closely examining a few cases can illuminate a phenomenon of growing significance.[86] Following the methodological approaches of Boggero and Kittrie, the sources for this inquiry include primary and

[81] John Gerring, "The Case Study: What It Is and What It Does," *The Oxford Handbook of Comparative Politics*, September 2, 2009, https://doi.org/10.1093/oxfordhb/9780199566020.003.0004.
[82] Maurer, *Cyber Mercenaries.*
[83] Swed and Crosbie, *The Sociology.*
[84] Lubin, *Selling Surveillance.*
[85] Bode and Huelss, *Autonomous Weapons.*
[86] Marco Boggero, *The Governance of Private Security* (Springer International Publishing, 2018), 68, https://doi.org/10.1007/978-3-319-69593-8.

secondary literature encompassing government policy briefs, peer-reviewed academic articles and books, media reports, statements from non-governmental organizations, and technical reports by cybersecurity companies. The relative transparency surrounding much of legal processes proves useful for this analysis; litigation and legislation generate substantial paper trails, and geopolitical developments grounded in legal justifications are often well-documented by governments.[87] This literature-based approach was complemented by insights from interviews with government officials, employees of PMSCs, in conjunction with domestic and international legal agreements.

Whereas international law situates states as the primary actors, corporate agency also remains central to this inquiry. In Part A, two sub-queries relevant to this research are explored: firstly, how PMSCs have legitimized themselves within the international system, and secondly, the practical, legal, and normative implications of outsourcing security functions to these corporations. These theoretical insights are corroborated with specific examples of corporate practice to illustrate how they interact with governments. In Part B, four multilateral initiatives undertaken within the last twenty years are evaluated for their efficacy in addressing the challenges presented by privatized security. The hard-law approach of the UN Draft Convention and Open-Ended Working Group is contrasted with the state-sponsored soft-law approach of the Montreux Document, the industry-driven soft-law approach of the International Code of Conduct for Private Security Service Providers, and the export control mechanism of the Wassenaar Arrangement. Drawing on Koskenniemian themes of normativity and concreteness, in conjunction of Hurd's conceptualization of law as inevitably empowering particular actors (as discussed in the literature review), each initiative is assessed based on its ability to encourage the crystallization of new principles to address the phenomenon of privatized security. Beyond evaluating the linguistic provisions of each document, and the negotiation process between various stakeholders, the case studies also contemplate domestic implementation and enforcement efforts. The comparative case study of multi-stakeholder

[87] Orde F. Kittrie, *Lawfare: Law as a Weapon of War* (Oxford: Oxford University Press, 2016).

initiatives reveals several implications of these initiatives in terms of their efficacy and legitimacy, and illuminates avenues for further research regarding this subject.

Analysis, Part A: Challenges of Privatizing Security

Part 1: Identifying Sources of Legitimacy and Authority

As described in the following sections, PMSCs have consolidated their legitimacy and authority in three ways: by invoking their status as security and risk experts, by emphasizing their efficiency as private actors in a neoliberal ideological environment, and by characterizing their services in a manner that differentiates them from "mercenaries", and does not impinge on "inherent state functions".

I. Security and Risk Experts

Risk management has become a central concept in contemporary security discourses across myriad actors and jurisdictions, both as a measure of insecurity and a discursive tool to justify the premeditation of risk and pre-emptive interventions. PMSCs have not only benefited from the growing demand for risk management —conforming to the functional needs of the market for force— but have also assumed a central role in perpetuating and manipulating this demand. Their framing of societal issues in a securitizing manner has enabled them to link their capabilities and expertise with previously identified sources of insecurity.[88] By developing logics and practices of risk identification, assessment and mitigation, PMSCs are able to create and sustain demand for the services they provide. Underpinning commercial risk analyses, profiling, and risk surveys is the 'expertise' of security professionals over the

[88] Tom de Groot and Salvador Santino F. Regilme, "Private Military and Security Companies and the Militarization of Humanitarianism," *Journal of Developing Societies*38, no. 1 (2021): 70, 73, https://doi.org/10.1177/0169796x211066874.

customer's personal experience of known dangers.[89] Krahmann considers how PMSCs generate demand and raise profits by constantly identifying new threats and increasing risk perception to expand the number of potential customers.[90] For instance, British firm G4S claims to use its "expertise in country threat assessments, coupled with… unique ground truth capability… [to] provide a full threat assessment across a number of destinations".[91] Following risk identification and assessment, PMSCs propose risk mitigation measures, offering reassurance by claiming to minimize their clients' alleged weaknesses and vulnerabilities.[92] GardaWorld (previously Aegis), for instance, affirms that their security solutions are "routinely reviewed to ensure continual improvement in… a rapidly changing security environment".[93] Drawing on the logic of "permanent precaution", these private actors justify the employment of extraordinary security measures to manage continually evolving threats.[94] These challenges are compounded in the digital realm, where governments lack the epistemic understanding that corporate actors possess regarding surveillance and cyber activities.

Furthermore, warfare's increasingly complex, technical nature has underwritten the growing demand for private qualifications and expertise that many state militaries have difficulty supplying independently. This trend has placed the security expert at the nexus of structures of power and knowledge. Private firms are often better equipped than national militaries, and are of particular relevance for countries involved in protracted, equipment-intensive operations like the US.[95] On the 'supply' side, PMSCs have emphasized the absence of reasonable alternatives by presenting themselves as security and risk experts qualified to

[89] Anna Leander, "The Power to Construct International Security: On the Significance of Private Military Companies," *Millennium: Journal of International Studies* 33, no. 3 (2005), 819, https://doi.org/10.1177/03058298050330030601.
[90] Cutler, "The Legitimacy," 178.
[91] G4S, *Intelligence and Advisory Services (IAS) Capability*, 4, https://www.g4sriskmanagement.com/-/media/g4s/riskmanagement/indexed-files/files/ias_protea_capability_-_final__-5_may.ashx?la=en&hash=385DA8129A45978CAF8A5B7195CEF19E.
[92] Joakim Berndtsson and Christopher Kinsey, *The Routledge Research Companion to Security Outsourcing* (New York, NY: Routledge, Taylor & Francis Group, 2016), 100.
[93] Berndtsson and Kinsey, *The Routledge*, 103.
[94] Liu, *Law's Impunity,* 103.
[95] Trevor Taylor, "Contractors on Deployed Operations and Equipment Support," *Defence Studies* 4, no. 2 (2004): 196, https://doi.org/10.1080/1470243042000325896.

compensate for an ineffective, expensive state sector incapable of fulfilling its security responsibilities.[96] State-clients on the 'demand' side, by purchasing their services, acknowledge and reproduce the PMSC's authority.[97] The "expert" status has generated a practical legitimacy for PMSCs, as states increasingly rely on their technologies and expertise for security governance purposes. Moreover, this anchoring of the PMSC's authority profoundly biases how contestation can be articulated, insofar as criticisms of PMSC's competence seems irresponsible and contrary to national security.[98]

II. Private Actors in a Neoliberal Environment

PMSCs gain authority not only through their expertise in providing security and risk-related services, but also by virtue of their status as private companies. Privatization refers to the "shifting of a function, either in whole or in part, from the public sector to the private sector".[99] Prior scholarship has linked military contracting to neoliberalism, a trend towards the increased outsourcing of traditionally governmental activities, and the assumptions associated with market efficiency.[100] A shared neoliberal discourse, underpinned by the belief that firms are more efficient than other economic agents, renders it more challenging to articulate critiques against PMSCs. In particular, the rapid and profound expansion of PMSC's influence has rendered them so central to many activities that some state-clients find it difficult to imagine carrying out military operations without the expertise they provide.[101] The authority that accompanies being a market actor biases the terms on which PMSCs are contested: the tendency towards market governance has rendered highly unorthodox contracting practices acceptable. No-bid contracts (awarded without reviewal of competing bids) and cost-plus contracts (with charges left open) coexist

[96] Prem, "Who Am I," 56.
[97] Weiss, "The Rise," 275.
[98] Anna Leander, "The Paradoxical Impunity of Private Military Companies: Authority and the Limits to Legal Accountability," *Security Dialogue* 41, no. 5 (2010): 475, https://doi.org/10.1177/0967010610382108.
[99] Lubin, *Selling Surveillance,* 37.
[100] Hilde van Meegdenburg, "What the Research on PMSCs Discovered and Neglected: An Appraisal of the Literature," *Contemporary Security Policy* 36, no. 2 (2015): 327, https://doi.org/10.1080/13523260.2015.1061755.
[101] Maurer, *Cyber Mercenaries,* 154.

with practices whereby companies write and control their own contracts.[102] The degree to which these practices are accepted and normalized is captured by the fate of attempts to criticize or redress them.

The diffusion of neoliberal norms into the realm of security has reinforced this dynamic: the conviction of the private sector's superiority as the more effective, cost-efficient alternative to the state-based provision of public services offers a normative rationale for privatizing previously "untouchable" aspects of government— including military and security services.[103,104] Whereas technical expertise empowers and authorizes private security providers, this trend is enabled through dominant ideological models favoring neoliberal norms of regulation and governance. Neoliberal economics emphasizes fiscal discipline, efficiency, and a reduced role for the state in the provision of services in favor of private actors.[105] This perspective has encouraged the adoption of new management strategies including voluntary codes of conduct, contracts, 'best practices', and other mechanisms of corporate self-regulation— which are transforming the conceptualization and delivery of security services.[106] Crucially, the resulting culture of economic efficiency has encouraged a shifting perception of security away from a public good supplied by states, towards a commodity sold by firms and available to anyone willing to pay.

The process of privatization has endowed PMSCs with an epistemic power over security discourses, implying that by consulting or lobbying policymakers, these companies can exert outsized influence over the regulation of the use of force.[107] As discussed in the previous section, the rise of outsourced security has signaled the rise of privately employed security "experts". They legitimize themselves by

---

[102] James Pattison, "The Challenge of PMSCs," *The Morality of Private War*, May 29, 2014, 4, https://doi.org/10.1093/acprof:oso/9780199639700.003.0001.
[103] Andreas Kruck, "Theorising the Use of Private Military and Security Companies: A Synthetic Perspective," *Journal of International Relations and Development* 17, no. 1 (2013): 7-9, https://doi.org/10.1057/jird.2013.4.
[104] Cutler, "The Legitimacy," 163,164.
[105] Singer, *Corporate Warriors*, 63.
[106] Cutler, "The Legitimacy," 162.
[107] Anna Leander, *Eroding State Authority? Private Military Companies and the Legitimate Use of Force*, 19, 2006, https://www.files.ethz.ch/isn/20511/Eroding_State_authority.pdf.

emphasizing the technical and managerial aspects of security, since their expertise is predicated on claims to technological competence and economic efficiency.[108] Increased reliance on PMSC experts has the tendency to displace security discussions outside the public realm, away from the legislative to a more restricted milieu where the executive, military, secret services, and PMSCs can define and manage issues. [109] Privatization and outsourcing are frequently explained by the value of secrecy and discretion in security matters, allowing decisionmakers to dispense with justifying military interventions to the public.[110] This trend is particularly salient when considering the sub-field of privatized intelligence: hiring PMSCs to collect and interpret intelligence endows them with the power to inform and organize the practical security agenda.[111] These companies can selectively determine the relevant information, and communicate to policymakers how they should interpret the information the firm provides. Although public actors may retain ultimate decision-making powers in managing security threats, their formal power loses salience if it is exercised in relation to an agenda largely controlled by private entities.[112]

III. Rhetorical Divestment from the Mercenary Label

Despite the challenge posed to PMSC's legitimacy by the concept of "inherently state functions", corporate actors have taken advantage of the evolving interpretation of the SMOV, characterized by a narrowing of the functions regarded as inherent to the state. In particular, they have accentuated their role in providing "defensive" and "security" functions to distinguish themselves from mercenaries, legitimizing themselves from the perspective of decision-makers. Both the SMOV and the anti-mercenary norm in international law share the ideal of centralized state control over the means of violence, and the

[108] Leander, "The Power", 824.
[109] Swed and Burland, "Outsourcing War," 9.
[110] This dynamic challenges decision-makers' accountability to their own citizens, and is further explored in a following section.
[111] S. Chesterman, "We Can't Spy ... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions," *European Journal of International Law* 19, no. 5 (2008): 1057, https://doi.org/10.1093/ejil/chn055.
[112] Leander, "The Power," Part 2.

political decision to maintain and deploy armed force. This has rendered illegitimate any violent actor not incorporated into the state structure. However, the anti-mercenary norm has significantly evolved since its initial codification. Historically, mercenaries were characterized as fighters participating in offensive or defensive combat, with only a tenuous affiliation to a group cause, and only minimally controlled by the state.[113] In recent years, by arguing that PMSC's use of force did not constitute combat —but rather, individual self-defense— advocates of PMSC legitimation created an alternative interpretation of the anti-mercenary norm framing PMSC practices as appropriate.[114] This shift was led not only by outcast or marginalized states, but rather, by leading members of the international system with the influence to dictate its legal and normative discourse— particularly the US, the UK and Germany. These actors have asserted that the SMOV refers to the control over the legitimate use of armed force, rather than its actual exercise.[115] The support by crucial actors including the UK Parliament, US Congress, UN Working Group on Mercenaries, and the UN Special Rapporteur on Mercenaries indicates the shrinking regulatory scope of the anti-mercenary norm.[116] Defensive force has become distinct from combat, such that PMSCs, insofar as they present themselves as providing defensive services only, do not violate the anti-mercenary norm and can be regarded as legitimate actors.

Given the transformation of the anti-mercenary norm, PMSC's ability to legally distance themselves from the stigma associated with "mercenaries" has played a central role in validating their activities. Taking advantage of the fading distinction between "combat" and "security" and the narrowing international understanding of "inherently governmental" functions, they have established their own discursive

[113] Elke Krahmann, "From 'Mercenaries' to 'Private Security Contractors': The (Re)Construction of Armed Security Providers in International Legal Discourses," *Millennium: Journal of International Studies* 40, no. 2 (2011), https://doi.org/10.1177/0305829811426673.
[114] Ulrich Petersohn, "Reframing the Anti-mercenary Norm: Private Military and Security Companies and Mercenarism," *International Journal: Canada's Journal of Global Policy Analysis* 69, no. 4 (2014), https://doi.org/10.1177/0020702014544915.
[115] Boggero, *The Governance,* 63.
[116] Petersohn, "Reframing the Anti-mercenary,", 491.

narrative that obscures and distracts attention from their most controversial services.[117] Prem describes the decoupling strategy pursued by PMSCs: even as they continue competing for lucrative security contracts and maintain armed security portfolios, they downplay their stakes in this business niche in favor of defensive operations.[118] This is especially prevalent in the context of cyber-intelligence companies, whose products can be employed for a range of offensive and defensive purposes. For example, Milan, Italy-based Hacking Team developed malware and offensive capabilities, releasing Remote Control System (RCS) in 2003.[119] Its consumer policy vowed to sell its services exclusively to government law enforcement and security services, and claimed that the company has internal guidelines to ensure its products are not misused.[120] The company marketed its technology as "an offensive solution for cyber investigations" intended to make "fighting crime… easy".[121] Similarly, Israel-based NSO Group developed the software application Pegasus, dubbed as military-grade spyware capable of hacking through the encryption on most cell phones and converting them into listening devices without the users' knowledge.[122] NSO's mission statement was "we work to save lives and create a better, safer world", and Pegasus was advertised as a tool for Western-aligned governments, police and spy agencies.[123] Little was known about NSO's client screening process other than an official statement that "our vetting process goes beyond legal and regulatory requirements to ensure the lawful use of our technology as designed".[124] Rhetorical divestment from an otherwise illegitimate line of military, combat-oriented services has enabled PMSCs to conduct business as usual.[125] A paradoxical situation has resulted where many current companies referred to as PMSCs have seemingly mitigated the perception that they operate in the offensive and protective business niches— while formally, they continue to provide these capabilities.

---

[117] Petersohn, "Reframing the Anti-mercenary Norm," 492.
[118] Prem, "The Regulation".
[119] Kim, "Global Export," 383.
[120] Maurer, *Cyber Mercenaries*, 37.
[121] Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control," *European Journal of International Law* 34, no. 3 (2023): 707, https://doi.org/10.1093/ejil/chad039.
[122] Kaster and Ensign, "Privatized Espionage," 355.
[123] Kaster and Ensign, "Privatized Espionage," 356.
[124] Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," *The New York Times*, January 28, 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.
[125] Prem, "Who Am I," 65.

This section has demonstrated that the combined effect of PMSC's status as *risk experts* and *private actors,* offering services *distinct* from those of traditional mercenaries, is to imbue these corporations with the economic logic and rhetoric necessary to legitimize their existence.

Part 2: Practical Challenges

Augmenting Capabilities, Yet Relinquishing Control

Rather than operating through formal state bodies, states have increasingly turned to corporate actors to indirectly actualize their geopolitical and security objectives— generating both factual and legal attribution difficulties.[126] According to Al Aridi, the use of proxy forces in the corporate sphere can provide governments with "plausible deniability", referring to covert activities against another state allowing the adversary to disclaim responsibility with a measure of credibility.[127] In contrast to traditional warfare's overt, clearly defined character, today's conflicts often entail states' covert involvement in conflict operations, achieved through their outsourcing of geopolitical objectives to private actors. Many proxies' operations enable plausible deniability by concealing the state beneficiary's identity; others — especially when considering non-kinetic cyber and intelligence operations— can operate clandestinely without their effects even being noticed.

The UN Working Group has consistently emphasized issues of institutional and contextual ambiguity as undermining PMSC regulation, particularly with reference to the concept of "direct participation in hostilities". From an institutional perspective, the Working Group's report notes that "under international humanitarian law, if private military and security contractors do not directly participate in hostilities, they

[126] Al Aridi, "The Problem," 173.
[127] Al Aridi, "The Problem," 147.

are considered civilians… however, the legal status of PMSC personnel performing functions closely linked to military operations, such as analyzing intelligence data, maintaining weapon systems, and resupplying forward-based forces, is less certain".[128] Unlike government military personnel, who are subject to the same laws regardless of their specific operational duties, PMSC personnel's accountability to domestic and international laws may be subject to the nature of their particular services.[129] In terms of contextual ambiguities, whereas PMSC personnel may be contracted to perform duties that are not "inherently governmental" functions and do not explicitly necessitate the deployment of armed force, these individuals may find themselves in chaotic combat environments where the line between acceptable activities (such as the defensive use of force) and the unacceptable becomes blurred.[130,131] Can the distinction between combat and providing security truly be maintained in the frail states in which asymmetric wars are frequently fought, and PMSCs are frequently employed?

As outlined in the practical examples below, by accessing the extensive resources and specialized expertise possessed by private firms, governments navigate a trade-off between enhancing their operational capacities, and relinquishing a degree of sovereign control.

Illustrative Example: The Wagner Group Introduces Security Liabilities for the Kremlin

Despite the possibility of achieving plausible deniability, the devolution of on-the-ground influence from public decision-makers to private actors involves considerable political and military risks for both PMSCs and their sponsors. Consider the case of the Wagner Group, a PMSC which frequently operates alongside Russian military forces, but has also been deployed to further the personal interests of clique of

[128] UN Human Rights Council, *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, report no. A/HRC/15/25/Add.3, Part II Art. 7, June 15, 2010, https://www2.ohchr.org/english/issues/mercenaries/docs/A-HRC-15-25-Add3_AEV.pdf.
[129] Swed and Crosbie, *The Sociology,* 77.
[130] Swed and Crosbie, *The Sociology,* 79, 91.
[131] Berndtsson and Kinsey, *The Routledge*, 174.

individuals surrounding Putin.[132] Wagner has progressively increased its autonomy from the Kremlin by securing contracts with its own Russian and foreign customers. For instance, in the Central African Republic, Sudan, and Mozambique, Wagner contractors were deployed to support the agenda of Russian business interests in natural resource extraction.[133] However, after entering into a contract with Syrian sponsors to capture a gas plant occupied by a Kurdish militia force and US military advisors, US air support was called in to repel the attack, leaving hundreds of the Russian Wagner forces dead or wounded.[134] This ill-advised operation encouraged the Kremlin to distance itself from the Wagner Group and tighten its control over PMSCs.[135] Insofar as entities such as Wagner are employed to advance the interests of particular political, economic, and military elites (rather than the central government itself) the political consequences arising from PMSC's independent initiatives may outweigh the geostrategic and economic advantages accompanying their use.

Illustrative Example: Reflex Ltd Undermines the United Arab Emirates' Plausible Deniability

The devolution of power to private actors has presented challenges in numerous contexts, Erik Prince's private military company Reflex Ltd was introduced to the Crown Prince and established itself in Abu Dhabi in 2010, with the ambition to create a force of commercial armed surrogates directly answerable to the Crown Prince. Designated as an 'elite counterterrorism unit', the battalion of mercenaries was intended to engage any 'terrorist' threat against the regime— a malleable term in the United Arab Emirates (UAE) which could refer to any entity that could potentially challenge the internal order in the Emirates.[136] Over the following decade, Reflex Ltd was renamed, rebranded, and expropriated from

[132] Åse Gilje Østensen and Tor Bukkvoll, "Private Military Companies – Russian Great Power Politics on the Cheap?," *Small Wars & Insurgencies* 33, nos. 1-2 (2021), https://doi.org/10.1080/09592318.2021.1984709.
[133] Jack Losh, "In Central Africa, Russia Won the War—but It's Losing the Peace," *Foreign Policy*, August 21, 2021, https://foreignpolicy.com/2021/08/21/in-central-africa-russia-won-the-war-but-its-losing-the-peace/.
[134] Eugenio Cusumano and Christopher Kinsey, "Concluding Comments," *Small Wars and Insurgencies* 33, nos. 1-2 (2021), https://doi.org/10.1080/09592318.2022.2021487.
[135] Losh, "In Central".
[136] Andreas Krieg, "The UAE's 'Dogs of War': Boosting a Small State's Regional Power Projection," *Small Wars & Insurgencies* 33, nos. 1-2 (2021): 160, https://doi.org/10.1080/09592318.2021.1951432.

Prince, who fell out with the Crown Prince. The first deployment of a Reflex Ltd subsidiary by the UAE government occurred in protection of the Emirati mercantilist grand strategy in Somalia in 2011 (establishing an anti-piracy force in Somalia's breakaway region of Puntland).[137] The so-called Puntland Maritime Police Force did not operate in the law enforcement realm or in a defensive security role, but rather, conducted lethal combat operations against targets on land and offshore.[138] However, the project was prematurely cancelled by the UAE because the operation —which was intended to provide the country not only with capacity and capability, but most importantly with discretion and deniability— became a reputational liability for Abu Dhabi.[139] This situation also illustrates how, if states operate too 'far' from proxies, proxies may become more likely to act independently, disobeying directives to execute their own financial or political motivations, and challenging the SMOV. Although externalizing the burden of warfare to a PMSC may prove cost-effective and obscure a state's involvement in a conflict, governments must also confront the risk that strategic and operational objectives may be actualized through unethical, illegal means, if at all.[140]

Attribution Challenges, Private Actors, and Technological Development

Whereas controlling proxy actors engaged in conventional military operations already entails challenges, ensuring cyber proxies' accountability introduces additional complexities. For a technology to act as an effective 'surrogate' to absorb the burdens of conflict traditionally allocated to state military personnel, it must facilitate the conduct of warfare discreetly, with plausible deniability before the international and domestic communities. [141] Activities pursued exclusively through CSTs are much easier to conceal (and thus unlikely to provoke significant domestic criticism), comparatively resource-efficient to execute in

[137] Matthew Cole, "The Complete Mercenary," *The Intercept*, May 3, 2019, https://theintercept.com/2019/05/03/erik-prince-trump-uae-project-veritas/
[138] Cole, "The Complete Mercenary".
[139] Kreig, "The UAE," 161.
[140] Andreas Krieg and Jean-Marc Rickli, *Surrogate Warfare: The Transformation of War in the Twenty-First Century* (Washington, DC: Georgetown University Press, 2019), 86.
[141] Krieg and Rickli, *Surrogate Warfare*, 86.

terms of manpower and materials, and even more difficult to trace back to government agencies than 'kinetic' proxies. Because the Internet allows for most cyber-operations to be launched from virtually anywhere worldwide, private contractors can engage in surveillance activities or even participate in an armed conflict overseas without leaving their home country.[142] The absence of geographic constraints in an increasingly nebulous "battlefield" complicates attribution to particular companies or individuals: it blurs the boundaries between providing technical and logistics support, versus conducting defensive or offensive cyber operations. For instance, a contractor undertaking reconnaissance activities at one moment could easily shift to digitally attacking a target network. [143] The potential to rapidly move between these roles demonstrates the synthesis of various functions traditionally characterizing private contractors' participation in conflicts. This dynamic corroborates the previously discussed insights of the UN Working Group— the ambiguity of contractor roles within a decentralized allows civilians to engage in activities that bring them increasingly closer to "direct participation in hostilities", without a commensurate degree of government oversight.

In this regard, cyberspace offers an ideal terrain for governments seeking plausible deniability, and commercial actors seeking to operate as instruments for covert action in exchange for profit.[144] It remains extremely challenging to promptly attribute malicious activity, in a manner that is independently verifiable and capable of withstanding public scrutiny.[145,146] Moreover, states' attribution potential remains asymmetric: whereas major geopolitical powers are gradually developing these proficiencies, such capabilities remain out of reach for smaller states. (Although they could receive assistance from more advanced powers, this practice requires significant trust, and non-trivial intelligence tradeoffs for

[142] Swed and Crosbie, *The Sociology*, 245.
[143] Maurer and Hoffmann, *The Privatisation,* 9.
[144] Cusumano and Kinsey, "Concluding Comments".
[145] Maurer, *Cyber Mercenaries*, 23.
[146] Mikael Weissmann et al., *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (London, United Kingdom: Bloomsbury, 2021), 119.

the information-sharing party).[147] Finally, increasing commoditization also renders it more difficult for individuals selling a product or service to have an insight into the end-use of a particular sale, removing one further potential source of attribution.[148] This dynamic further increases spyware transactions' anonymity, facilitating the use of these capabilities by states and further blurring lines of responsibility. The capabilities necessary to address attribution problems —as not merely a legal concern, as previously discussed, but a practical one— are asymmetric and frequently unavailable within the time frame that decision-makers may need to act expediently in national security contexts.

Illustrative Example: NSO Group Evades Multilateral Accountability Mechanisms

Furthermore, the privatized security industry's opaqueness and complexity renders it extremely difficult for members of the international community to form judgments on particular issues. In the case of cyber-intelligence and spyware companies in particular, attribution is further undermined by the fact that these entities are routinely bought and sold, allowing them to perpetually relocate, rebrand, and restructure themselves.[149] Consider the case of NSO Group, an Israeli cyberespionage technology firm valued at over US$1 billion in November 2021.[150] The firm had developed the software application Pegasus, dubbed as military-grade spyware capable of hacking through the encryption on most cell phones and converting them into listening devices without users' knowledge.[151] In December 2021, facing mounting bilateral pressure from allies (primarily the US and France), the Israeli Ministry of Defense announced the strengthening of regulations on export controls. These new restrictions included reducing the number of countries to which spyware companies can potentially sell their products, from 110 to only 37.[152] The significant decline in prospective buyers was economically detrimental to many Israeli spyware

[147] Maurer, *Cyber Mercenaries*, 24.
[148] Riecke, "Dual-Use," 716.
[149] Lubin, *Selling Surveillance*, 12.
[150] Lubin, *Selling Surveillance,* 3.
[151] Sean D. Kaster and Prescott C. Ensign, "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware," *Thunderbird International Business Review*65, no. 3 (2022): 355, https://doi.org/10.1002/tie.22321.
[152] Bergman and Mazzetti, "The Battle".

companies, most famously NSO Group. However, NSO (among approximately 29 other companies), simply relocated to Cyprus, characterized by relaxed export controls.[153] PMSCs possess remarkable evasion capabilities, often re-naming themselves between jurisdictions, and are constantly bought and sold under alternative entities. Like other companies, NSO went by various names in foreign countries such as Q Cyber Technologies (Israel), OSY Technologies (Luxembourg), and Westbridge (North America). This contributed to the company's ability to evade legal accountability while operating in multiple jurisdictions (and allow its clients to retain plausible deniability). [154]

Illustrative Example: Hacking Team Data Leak Enables Attribution to State Actors

The exploits of Milan-based Hacking Team (HT) also illustrate the difficulty of regulating cyber-surveillance companies under international law. In 2014, hacktivist Phineas Fisher leaked over 400 gigabytes of HT's most sensitive data, including internal emails, client exchanges, and most of the company's source code and zero-day exploits.[155] Hacking team clients were revealed to include law enforcement and security agencies across Egypt, Nigeria, Oman, India, Mexico, Morocco, Ecuador, Russia, Italy, Hungary, the US, and Switzerland, among others.[156] The leaked documents also revealed that, contrary to the company's claims, HT undertook only the most superficial vetting of clients and contractors, and cultivated extensive negotiations with state security agencies accused of human rights violations.[157] For example, although HT denied that it had ever conducted business with Sudan —which was under a UN arms embargo— an invoice for 480,000€ to the Sudanese security service was unearthed. [158] In response, HT claimed that its programs were sold in Sudan prior to the regulation of dual-use technologies.[159] The data leak also revealed that the United Arab Emirates paid Hacking Team 634,500

[153] Lubin, *Selling Surveillance,* 13.
[154] Kaster and Ensign, "Privatized Espionage," 358.
[155] Kim, "Global Export," 383.
[156] Riecke, "Unmasking the Term," 708.
[157] Maurer, *Cyber Mercenaries*, 79.
[158] Burkart and McCourt, "The International," 47.
[159] Burkart and McCourt, "The International," 47.

USD for the use of its products, with which they surveilled over 1,000 people, including political dissidents and journalists.[160] HT relied on numerous zero-day exploits for its products, but following the data leak, its library of zero-days was disclosed and employed by malicious threat actors worldwide.[161] The data leak of HT foregrounds a central reason why international norms often fail to prevent security breaches by non-state actors: states have an inherent interest in maintaining their distance from proxies. The more substantive the relations between a state and a proxy, the more likely the regime is to be exposed if the proxy is caught.

As demonstrated by these examples, it is common corporate practice to exploit legal discrepancies in national export controls and licensing procedures, by relocating business and changing distribution lines to states with more lenient rules.[162] Moreover, establishing evidentiary links between states and companies has become incredibly challenging: only through deliberate data leaks is the information necessary to hold actors responsible revealed.

Accountability Challenges Between Governments and Citizens

Finally, the 'outsourcing' of security to private actors introduces accountability challenges not only between governments and PMSCs, but also between governments and their own citizens. War has become a permanent state of affairs requiring leaders' ongoing commitment to maintain their strategic interests. Whereas large-scale deployments and major combat operations are politically ill-suited to conflicts with ambiguously defined objectives against intangible threats, PMSCs acting as proxies can provide discreet military options outside the public's purview.[163] In particular, the Executive can unilaterally carry out military policy and employ violence overseas, without having to fully disclose the

[160] Maurer, *Cyber Mercenaries*, 79.
[161] Fidler, "Regulating the Zero-Day," 469.
[162] Lubin, *Selling Surveillance,* 12.
[163] Krieg and Rickli, *Surrogate Warfare*, 77.

strategic and operational costs to citizens.[164] The governments employing PMSCs are not directly accountable for PMSC's behavior and its implications in the same way they are responsible for the actions of the state's armed forces. If a PMSC is found to be guilty of gross misconduct, governments can distance themselves from the company in a way that is not possible when considering their own militaries. Whereas the deployment of a state's own military forces remains a public and publicized phenomenon in many countries, the secret use of PMSCs circumvents the primary avenues through which citizens are informed— depriving them of the ability to register their approval or voice their misgivings regarding their state's involvement in conflict.[165,166] Beyond traditional PMSC's role in the tangible execution of security operations, PMSCs possessing spyware and intelligence capabilities play an increasing role in strategic decision-making regarding a conflict.[167] By shaping the security and strategic perceptions of government agencies, these actors can gain epistemic influence over the making of foreign policy itself, amplifying the domestic accountability challenges previously identified.

Concluding Insights

This section demonstrated that in some ways, PMSCs offering cyber and intelligence capabilities in the digital realm merely constitute an extension of the existing practice of outsourcing functions to traditional PMSCs. Both types of corporate actors legitimize themselves through similar mechanisms: invoking their status as risk experts and private actors in a neoliberal, privatization-friendly environment, and rhetorically divesting themselves from the "mercenary" term (by virtue of the diverse non-combat services they provide). However, the confluence of unprecedented technological development and privatization in the cyber and intelligence realms exacerbates the challenges of responsibility and

[164] Jon D. Michaels, "Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War," *Washington University Law Review* 82, no. 3 (2004): 1078, https://openscholarship.wustl.edu/law_lawreview/vol82/iss3/6.
[165] Krieg and Rickli, *Surrogate Warfare*, 71.
[166] Michaels, "Beyond Accountability," 1079, 1080.
[167] S. Chesterman, "We Can't Spy".

attribution already identified with regards to PMSC activities. As illustrated by the examples of the Wagner Group and Reflex Ltd, policymakers face a tradeoff in conflict environments between the strategic and operational benefits of achieving "plausible deniability", and the disadvantages associated with partially relinquishing of sovereign control. This compromise is also evident in the activities of NSO Group and Hacking Team: cyber-intelligence PMSCs can generate plausible deniability for state-clients through their clandestine, cross-jurisdictions activities, yet they also become a liability for states when their operations are revealed. Finally, the kinetic power of traditional PMSCs allows governments to engage in protracted, resource-intensive conflicts while evading domestic political scrutiny, while the intelligence collection and analysis abilities of cyber-intelligence PMSCs can increasingly influence leaders' policy decisions while circumventing traditional accountability structures.

Analysis, Part B: Multilateral Initiatives

Having identified and explored several challenges the international community must confront given the increasing prevalence and legitimacy of states' hiring PMSCs, this section contemplates the efficacy of multilateral initiatives seeking to understand and regulate the contemporary privatization of warfare. Several developing initiatives aimed to regulate PMSCs have situated contractual, multi-stakeholder strategies as the centerpiece of their efforts. This section explores a legally binding initiative (the UN Draft Convention), two soft-law multi-stakeholder initiatives (the Swiss Initiative and the ICoC), and an export control regulation (the Wassenaar Arrangement).

Since the 1990s, multi-stakeholder initiatives (MSIs) have become an increasingly prominent mode of regulation across myriad sectors and issue areas.[168] They allow states to cooperate on globally relevant

[168] Klaus Dingwerth and Philipp Pattberg, "World Politics and Organizational Fields: The Case of Transnational Sustainability Governance," *European Journal of International Relations* 15, no. 4 (2009): 708, https://doi.org/10.1177/1354066109345056.

issues in nonbinding contexts, allowing flexibility and fewer formal limits on sovereignty.[169] PMSCs have not been immune to this trend, as evidenced by the following case studies bringing together representatives from states, civil society, and PMSCs in international fora. Proponents of MSIs assert that these initiatives can encourage effective industry governance; there exists a normative appeal in the deliberative, consensual character allowing for participation by a wide range of stakeholders, and in the ability for problem-solving through concerted action.[170] However, one must also recognize that MSIs do not only promote free and unrestrained action: new methods of security governance are not necessarily less hierarchical and more inclusive than traditional state-based forms of political regulation.[171] Exercises of power, although not defined in terms of coercion or overt conflict, may nonetheless be inherent in MSIs. Power refers to "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate".[172] MSIs differentially enable and constrain their participants to partake in governing the PMSC industry, as actors strategically select policy venues to advance their objectives. In the context of this inquiry, influential states have pursued the strategies of *forum shifting* (diverting attention from a status quo institution to another that would better serve their interests), *forum creation* (establishing a competing institution), and *forum blocking* (undermining a forum's legitimacy to promote an agenda that threatens their interests).[173] For each initiative, a description of the conditions motivating its emergence, its core principles, and its objectives underpins a subsequent examination regarding the negotiation of provisions, and their local implementation.

[169] Prem, "The Regulation," 345.
[170] Deborah D. Avant, "Pragmatic Networks and Transnational Governance of Private Military and Security Services," *International Studies Quarterly* 60, no. 2 (2016), https://doi.org/10.1093/isq/sqv018.
[171] Oliver Westerwinter, "Bargaining in Networks," *The New Power Politics*, August 1, 2016, 222, https://doi.org/10.1093/acprof:oso/9780190604493.003.0008.
[172] Prem, "The Regulation," 347.
[173] Julia C. Morse and Robert O. Keohane, "Contested Multilateralism," *The Review of International Organizations* 9, no. 4 (2014), https://doi.org/10.1007/s11558-014-9188-2.

Case Study: UN Working Group and Draft Convention

Initiative Emergence, Core Principles and Objectives

PMSC's appearance in the international milieu has reinvigorated international regulatory discussion within the UN, manifest as the UN Working Group on the Use of Mercenaries (a collective body encompassing five independent experts, representing five geographical regions). Acknowledging that the UN Mercenary Convention was of limited application for regulating PMSCs, the Working Group's mandate was to monitor and assess the impact of new manifestations of PMSC's activities, and draft international basic principles to encourage respect for human rights by these companies.[174] This process culminated in the UN Draft International Convention on the Regulation, Oversight, and Monitoring of Private Military and Security Companies in 2010, in conjunction with the establishment of the Intergovernmental Open-Ended Working Group (OEWG) by the Human Rights Council (HRC) in 2010.[175] The OEWG focuses specifically on "reaffirm[ing] and strengthen[ing] State responsibility for the use of force," especially by "identify[ing] those functions which are inherently governmental and which cannot be outsourced".[176] The organization's proposed Draft attempted to reconcile the polar positions on regulation and criminalization, defining a PMSC as "a corporate entity which provides on a compensatory basis military and/or security services by physical persons and legal entities".[177] Advocating for the reinstatement of the SMOV and stressing the risks posed by the proliferation of privatized warfare, the document would have forbade the personnel of PMSCs from using force.[178] Moreover, the draft articles proposed various enforcement measures including the reinstatement of a PMSC governance regime including licensing, due diligence duties, international oversight mechanisms, and civil and criminal

[174] Prem, "The Regulation," 354.
[175] Boggero, *The Governance*, 63.
[176] UN Working Group on the Use of Mercenaries, *Draft Convention*, Art. 1.
[177] UN Human Rights Council, *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, report no. A/HRC/15/25, Art. 2(a), July 5, 2010, https://digitallibrary.un.org/record/688383?ln=en.
[178] UN Human Rights Council, *Report of the Working Group*, Art. 8.

sanctions in the event of violations of domestic or international law (particularly IHL and IHRL).[179] Because the HRC has historically taken a critical view of private force, it is no coincidence that the Draft Convention represents the perspectives of states reluctant to legitimize PMSC's large-scale employment.[180] In endeavoring to create a legally binding instrument, the Draft Convention pursues an objective beyond any other international instrument in addressing PMSC activities.

The Draft Convention's strength lies in its accountability and transparency mechanisms. The Working Group specifically proposed an international court of arbitration governed by a "Code" to provide a formal dispute mechanism for issues arising from PMSC activities; this arrangement would directly provide binding obligations to these companies and their contractors.[181] At the international level, the Draft Convention provides for an Oversight Committee, empowered to receive petitions and operate an inquiry procedure— thus empowering aggrieved individuals and groups to make claims that their rights provided for under the Draft Convention have been violated.[182] These international enforcement frameworks are complemented by articles within the Draft Convention requiring would-be States Parties to enact specific offenses under their domestic law, establish jurisdiction over offences, and fulfill obligations regarding prosecution or extradition.[183]

Disproportionate Influence of Powerful Actors

Despite garnering support from Russia, China, and most developing countries on the HRC, from its inception the efforts of the Working Group and its successor (the OEWG) were met with resistance both by industry representatives and prolific users and suppliers of PMSC services— particularly the US, the

[179] UN Working Group on the Use of Mercenaries, *Draft Convention*, Part I Art. 2(d), Art. 2(e), Part II Art. 7(2), Part IV Art. 19, Part V Art. 29.
[180] White, "Outsourcing Military," 150.
[181] Liu, *Law's Impunity*, 319.
[182] Boggero, *The Governance,* 70.
[183] UN Working Group on the Use of Mercenaries, *Draft Convention*, Part IV Arts. 19-24.

UK, and the European Union. The UN process' consensual, all-inclusive approach and variety of dissenting voices within the HRC diluted these actors' overall influence, who were anxious to retain their flexibility in PMSC employment.[184] Favoring a soft-law approach legitimizing these companies' usage, and anticipating mounting regulatory activity from the UN, the US, UK, and EU pursued the two complementary strategies of *forum blocking*, described below, and *forum shifting* (to the Swiss Initiative from which the Montreux Document and ICoC emerged, discussed in a subsequent section).[185] In this context, *forum blocking* refers to Western governments' repeated attempts to obstruct the Working Group's and OEWG's activities by voting against their mandate and recommendations. For example, during debates in the HRC following the Draft Convention's submission, delegates from the US and the UK objected to the Draft Convention. They disputed the Working Group's competence on the grounds that PMSCs "could not be considered mercenaries"; the resolution's repeated use of the term "mercenary" in relation to PMSCs was regarded as a source of concern that would impede collaboration on regulatory issues.[186] Opposition to the Draft Convention was also predicated on the "impracticality" of a future UN Convention's legally binding character, and the HRC's questionable appropriateness as a forum for addressing PMC regulation.[187,188] Eventually, the resolution inaugurating the OEWG was passed without Western states' support, who pivoted their focus to the Swiss Initiative (and eventually the ICoC) which more closely reflected their interests.[189] Ultimately, the Draft Convention was not adopted given the pressure from economically advanced states where PMSCs are incorporated (especially the UK, US, and

[184] Mumford's analysis reveals Western governments' increasing dependence on private-sector assistance. The United States in particular is arguably reliant on the industry to an extent that engaging in warfare without PMSCs has become practically infeasible.
Andrew Mumford, "Proxy Warfare and the Future of Conflict," *The RUSI Journal* 158, no. 2 (2013), https://doi.org/10.1080/03071847.2013.787733.
[185] For further information regarding forum blocking and shifting, see Morse and Keohane, "Contested Multilateralism".
[186] Sorensen, "The Politics," 97.
[187] These actors asserted that "certain legal issues", notably state responsibility, included within the Draft Convention were outside the HRC's purview.
[188] Prem, "The Regulation," 355.
[189] J. Cockayne, "Regulating Private Military and Security Companies: The Content, Negotiation, Weaknesses and Promise of the Montreux Document," *Journal of Conflict and Security Law* 13, no. 3 (2008): 423, https://doi.org/10.1093/jcsl/krp006.

France).[190] This failure illustrates how powerful political actors' ulterior interests have restricted the development of binding international laws to regulate PMSC activity.

Definitional Ambiguities and Linguistic Amendments

Although the objective of generating a hard-law mechanism through the Draft Convention and the OEWG had (until recently) prevailed within the UN, such an instrument would have severely limited the functions permitted to be contracted out to PMSCs. The Draft Convention adopts an extremely broad interpretation of "inherent state functions" based on the principle of the state's monopoly on the legitimate use of force— which, as previously described, is itself extremely contested within the international community in the context of privatized warfare.[191] In the Convention, "inherently state functions" include not only "direct participation in hostilities, waging war and/or combat operations, [and] taking prisoners" but also extend to "law-making, espionage, intelligence, [and] knowledge transfer with military, security, and policing application".[192] As a result, actors including the US, who outsource their spying and intelligence activities to private contractors in considerable numbers, do not endorse the Draft Convention.[193] These tensions reflect on-the-ground realities which the Draft Convention's language seems to ignore.[194] The situation is emblematic of the fundamental challenges proposed international laws encounter in navigating a compromise between precision and relevance. Although admirable restrictions in theory, if enacted, these limits would have amounted to nothing less than a partial ban on PMSC activities, which is simply unrealistic.

---

[190] Boggero, *The Governance*, 68.
[191] Boggero, *The Governance*, 66.
[192] UN Working Group on the Use of Mercenaries, *Draft Convention on Private Military and Security Companies (PMSCs)*, report no. A/HRC/WG.10/1/2, Art. 2(i), May 13, 2011, https://digitallibrary.un.org/record/707162?ln=en&v=pdf#files.
[193] Chesterman, "We Can't Spy," 1056.
[194] Huskey, "Accountability for Private."

The broad definition of PMSCs adopted by the Working Group contributed to the elimination of the "mercenary" label from its reports because it implied that, irrespective of their motives or actions, PMSCs did not constitute mercenaries. This linguistic amendment rendered it possible to increasingly delimit the types of actors and services that should be criminalized By replacing the concept of "mercenary activities" with "PMSCs" and "inherently state functions" within its discourse, the Working Group created the possibility of legalizing companies selling armed force in conflicts for profit, through "improved" state regulation.[195] Whereas the legal definition of "mercenary" has remained static, the Draft aligns with the normative evolution of "mercenary" since its initial institutionalization (as described earlier in the analysis). Rather than reflecting the use of armed force by non-state actors in inter- and intra-state relations, the norm is now widely regarded by state actors as proscribing only direct participation by non-state actors in combat.[196] In 2010, the UN Draft Convention on PMSCs drew the seemingly logical conclusion from this changing discourse by suggesting that even the direct participation of PMSCs in hostilities should only be prohibited in a limited set of circumstances, and instead proposed the regulation and licensing of these firms and their services.[197] Ultimately, this shift from the *actor* to certain illegal *activities* has created a discursive space for the legalization of the use of armed force by profit-motivated corporate actors.

Participation and Enforcement Challenges

As previously discussed, states can increase the probability that negative actions by PMSCs are regarded as outliers in the international community (rather than establishing a pattern of normalized behaviors) by implementing strong accountability mechanisms. However, a Working Group report highlighted that even states possessing the *capacity* to domestically enact and enforce the monitoring and redress protocols for

[195] Krahmann, "From 'Mercenaries,'" 362.
[196] Petersohn, "Reframing the Anti-mercenary," 487.
[197] Krahmann, "From 'Mercenaries,'" 360.

which the Convention provides often have not done so in practice.[198] As a substantive example, a dearth of internal oversight and inadequate inter-agency coordination resulted in the US Government being unable to provide the Working Group with comprehensive data on PMSC usage.[199] Lacking any form of centralized PMSC accountability mechanisms, the Government has actually resorted to contracting out oversight to PMSCs themselves. In Afghanistan, for example, the Armed Contractor Oversight Division is responsible for investigating and reporting incidents involving the use of force.[200] When private contractors operate in disparate locations, often lacking dedicated military supervisors and a defined chain of command, their performance as profit-seeking surrogates is not scrutinized. [201,202] The lack of quality control in overseeing the externalization of military and security services undermines has undermined the government's ability to investigate allegations of wrongdoing, and prosecute illegal PMSC activities.[203] The UN initiative's viability and legitimacy is predicated on the assumption that that states possess the capacity and willingness to implement such a convention, including the establishment of comprehensive domestic regulation and oversight regimes. Yet when considering state practice, PMSC accountability remains elusive.

Case Study: Montreux Document (MD)

Initiative Emergence, Core Principles and Objectives

Despite allegations of PMSC misconduct, industry regulation has long proven elusive given ambiguities regarding which laws —if any— applied to them, and to which actor legal responsibility for their conduct

[198] United Nations General Assembly, *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, report no. A/HRC/15/25/Add.3, 9, June 15, 2010, https://documents.un.org/doc/undoc/gen/g10/143/85/pdf/g1014385.pdf?token=ZcthrtcwHisjOga0eq&fe=true.
[199] Swed and Crosbie, *The Sociology*, 79.
[200] United Nations General Assembly, *Report of the Working Group*.
[201] Swed and Crosbie, *The Sociology*, 80.
[202] Cusumano, *Mobilization Constraints*, 86.
[203] Krieg and Rickli, *Surrogate Warfare*, 127.

could be attributed. The Montreux Document (MD) constituted the first international attempt to articulate state responsibilities regarding the operation of PMSCs in an armed conflict environment. It emerged from a joint initiative sponsored by the Swiss Foreign Ministry and the ICRC in 2005 to reiterate the principles and rules under IHL and IHRL applicable to PMSCs operating in armed conflict zones.[204] Although essentially state-driven, the Swiss Initiative benefited from the input of other stakeholders (including international organizations, industry representatives, academics, and civil society groups) who were consulted during four expert meetings between January 2008 and April 2008.[205] Consensus emerged among these actors that PMSCs do not in fact operate in a legal vacuum, but rather, that states, PMSCs and individuals "are all subject to quite extensive international legal obligations".[206] The outcome of these meetings, the MD, was endorsed by 17 states in September 2008.[207] Following the state-centric nature of international law, the MD makes a significant and unique contribution in its approach to law and practice by outlining the responsibilities of three relevant entities: Contracting states (those hiring PMSCs), Territorial states (countries on whose territory PMSCs operate), and Home states (countries in which PMSCs are based).[208] Part 1 recalls "pertinent legal obligations" applicable to PMSC (outlining treaty and principle norms), and attempts to clarify the legal concepts of "state responsibility" and "due diligence" as they relate to PMSCs.[209] Part 2 outlines "good practices" for PMSCs and state conduct as it relates to PMSCs (encompassing principle and policy norms).[210] The MD diverges from the UN Draft Convention in that its primary purpose is to restate and reconsider existing legal obligations and practices in a new context (PMSC operation in armed conflict environments), rather than creating new ones. Ultimately, the MD does not impose any new constraints upon states exceeding the commitments previously made.

[204] Boggero, *The Governance*, 46.
[205] Prem, "The Regulation".
[206] Cockayne, "Regulating Private," 418.
[207] Swed and Crosbie, *The Sociology,* 184.
[208] Berenike Prem, *Private Military and Security Companies as Legitimate Governors: From Barricades to Boardrooms* (London, United Kingdom: Routledge, 2020), Chap. 6.3.2.
[209] Huskey, "Accountability for Private," 204.
[210] Sorensen, "The Politics," 103.

Exclusion of Non-Governmental Actors

Drafting attempts were complicated by the apparently contradictory negotiating positions of two different groups. One group, including the US (joined at various points by Australia, the UK, and Canada) sought to reduce the prominence of human rights language in the draft text, given its focus on armed conflict.[211] This group also expressed skepticism regarding the extraterritorial reach of obligations engendered in human rights conventions, and called for clarification of states' due diligence obligations (with the result that this terminology was eventually removed from the document). A second group including the ICRC and Amnesty International advocated stronger human rights language, particularly with respect to states' due diligence, prevention, and remedial obligations under IHRL.[212] States agreed to finalize the document through continuous written consultations, ultimately excluding non-governmental actors to generate an "intergovernmental" statement.[213] This approach antagonized non-governmental actors, who had remained extensively involved in earlier stages of a working draft's development. Some organizations questioned whether they had simply been brought into the negotiations as a triangulating tactic, since their inclusion represented the ICRC perspective as more 'moderate' (facilitating increased state support for that position).[214]

Normalizing and Legitimizing PMSCs

In contrast to the Draft Convention, the MD displays an extremely broad understanding of the transferable responsibilities of states to PMSCs, which entails a narrow interpretation of the SMOV. To some degree, this emanates from political necessity: a comprehensive definition of military and security functions was required to secure the consent of participating states including the US and the UK, who have very

[211] Cockayne, "Regulating Private," 421.
[212] Cockayne, "Regulating Private," 409.
[213] Liu, *Law's Impunity,* 309.
[214] Cockayne, "Regulating Private," 424.

permissive cultures of security outsourcing.[215] Law can serve a subtle legitimizing function by shifting the terms of the debate on actors who sell armed force in conflicts from "mercenaries" to "PMSCs". Whereas the Working Group characterized PMSCs as a new variety of mercenaries, the MD does not reference mercenarism as it pertains to PMSCs, but rather, views PMSCs as a distinct phenomenon.[216] Despite its declared intent of neutrality, the MD expresses signatory states' desire to employ and regulate, rather than criminalize and ban these companies.[217] This is reflected in the presumed "neutral" label selected for private military and security operators ("PMSCs"), situating these firms beyond the mercenary/combatant debate and its negative historical connotations. Starting from the premise that PMSCs are relatively unproblematic insofar as they align with IHL, the Montreux Document reifies the contracting trends of recent years in an apparently unquestioned manner. By accepting PMSCs as an indisputable "given" within international politics and endeavoring to pragmatically regulate them, the MD normalizes and empowers these actors, while foreclosing the imagination of alternative approaches.

The Dilution of Existing International Law

The MD's penultimate draft garnered significant criticism from Amnesty International and the International Commission of Jurists, who asserted that "the current draft falls short, in substantial respect' of the Swiss Initiative's stated goal of clarifying state and PMSCs obligations".[218] Their statement appears to have minimally impacted the final MD: the final September 2008 version contained numerous of linguistic changes designed to underscore the document's largely hortatory nature, further marginalizing the human rights perspective within the text. Passages were introduced at the beginning of each section emphasizing the document's non-binding nature, and repeated caveats were introduced regarding the extent of states' treaty and customary obligations ("within their power", "effective [control]", "as widely

[215] Prem, *Private Military,* 6.3.2.
[216] Marie-Louise Tougas, "Some Comments and Observations on the Montreux Document," *Yearbook of International Humanitarian Law* 12 (December 2009): 323, https://doi.org/10.1017/s1389135909000129.
[217] Prem, *Private Military*, 6.3.1.
[218] Cockayne, "Regulating Private," 423.

as possible", "specific circumstances") in order "to make clear that States are not obliged to do what they are unable to do".[219] Additional changes to the legal language had even more significant implications: Part One, Article 18 addressing the obligations of all states was revised to remove language from the Geneva Conventions indicating an obligation to "exert their influence, to the degree possible, to prevent and end violations, either individually or through multilateral mechanisms, in accordance with international law".[220] Draft provisions for each of the contracting, territorial and home states, suggesting that it is good practice for states to consider the potential impact of hiring, licensing or permitting the activities of a specific PMSC on the operating environment, were also deleted.[221] Seiberth notes that the MD's approach in affirming existing international law is "conservative with respect to state responsibility" and "incomplete by omitting extraterritorial jurisdiction of human rights and due diligence obligations".[222] This implies that the Document has failed to effectively clarify the pertinent legal obligations applicable to private military and security companies under IHL and HRL.

From Human-Rights and Victim-Centric to Contractual and State-Centric

One additional embedded amendment may have significant long-term implications on the MD's potential to operate as a basis for effective human rights accountability arrangements regarding PMSC's misconduct during warfare. During the final consultations in 2008, the document's language was subtly reoriented away from victims' rights to remedies to harms suffered, toward a more legalist orientation predicated on states' formal responsibilities to provide a remedy. For instance, one obligation of contracting states was rephrased from "provid[ing] effective measures *for harm caused by* the conduct of

[219] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part 1.A, Art. 4; Part 1.B, Arts. 9, 13.
[220] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part 1, Art. 18.
[221] Cockayne, "Regulating Private," 417.
[222] Corinna Seiberth, *Private Military and Security Companies in International Law: A Challenge for Non-binding Norms: The Montreux Document and the International Code of Conduct for Private Security Providers* (Cambridge, UK: Intersentia, 2014), 159.

PMCSs and their personnel" to "provid[ing] effective measures *for relevant misconduct* of PMSCs and their personnel".[223] The ambiguities concerning how "relevance" and "misconduct" could be tangibly measured narrow the state's apparent remedial obligations. A similar shift was achieved by revising the good practice for contracting states in PMSC selection from considering "the financial and economic capacity of the PMSC, including *whether it can demonstrate access to adequate financial resources allowing for compensation for individuals injured by the PMSC or its personnel",* to considering "the financial and economic capacity of the PMSC, including *for liabilities that it may incur"*. [224] This evolution from a victim-centric to a state-centric perspective is unsurprising, given non-state actors' exclusion from the negotiation's final stages.

Furthermore, where contractual provisions express or incorporate external legal obligations, as in the MD, there exists a possibility for the reduction or dilution of legal terms. This is evident in two of the MD's suggestions as "good practices" for contracting States. Firstly, to "determine which services may or may not be contracted out to PMSCs" merely provides for the guidelines for determining such boundaries, rather than imposing concrete limitations.[225] By contrast, Article 9 of the Draft Convention (analyzed in the previous section) requires States parties to "*specifically prohibit* the outsourcing to PMSCs of functions which are defined as inherently State functions", and enumerates particular prohibitions on PMSC activities.[226] Secondly, the MD suggests that states "include contractual clauses and performance requirements that *ensure respect* for relevant… international humanitarian law and human rights law by the contracted PMSC".[227] The Draft Convention instead requires that State parties "take legislative,

[223] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part 1.A, Art. 4.
[224] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part 2.A.III, Art. 7.
[225] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part 2.A.I.
[226] UN Working Group on the Use of Mercenaries, *Draft Convention,*, Article 9.
[227] International Committee of the Red Cross and Swiss Federal Department of Foreign Affairs, *The Montreux Document*, Part IV, Art. 14.

judicial, administrative and other measures as may be necessary to ensure that PSCs and their personnel are *held accountable* in accordance with this Convention and to ensure respect for and protection of international human rights and humanitarian law".[228] In contrast to contract law's myopic, inward-looking nature, human rights law purports to express universal, inalienable rights (and confers them without imposing concomitant obligations).[229] Additionally, whereas human rights law is restrictive in establishing normative boundaries for acceptable treatment, contract law is enabling—rendering it "non-judgmental and limitless".[230] Juxtaposing the contractually-oriented MD with the human-rights centric Draft Convention foregrounds the inadequacies of collapsing human rights protections within contract law mechanisms.

Enforcement Challenges

Despite restating the existing international legal obligations towards private military corporations, contracting states, and host states (such that it contains elements of hard law) the MD remains a non-binding international treaty. Although an earlier draft prepared by the ICRC and the Swiss government envisioned a binding treaty, it was abandoned under pressure from numerous states— notably the US, UK, and Canada.[231] The Montreux Document highlights a structural challenge associated with outlining preventative responsibilities under international law: the articulation of bare-minimum standards renders their application to novel situations severely circumscribed.[232] Amnesty International criticizes the MD's "international law section… [which] does not elaborate with enough detail and precision the applicable international law… limiting its utility either as guidance to States and [PMSCs] regarding their existing legal obligations".[233]

---

[228] UN Working Group on the Use of Mercenaries, *Draft Convention,* Article 5.
[229] UN General Assembly, *Universal Declaration of Human Rights*, report no. UNGAR 217 A(III), Preamble, 1948.
[230] Liu, *Law's Impunity,* 212.
[231] Prem, "The Regulation," 355.
[232] Seiberth, *Private Military*, 156-60.
[233] Amnesty International, *Amnesty International Public Statement on the Montreux Document*, 2, October 14, 2008, https://www.amnesty.org/en/wp-content/uploads/2021/07/ior300102008en.pdf.

Moreover, the Document demonstrates the weakness inherent in establishing productive responsibilities: despite recommending home States to establish authorization systems, the UK disregarded this provision and instead opted for a government-based, self-regulatory system.[234] As illustrated by the UK's efforts to enforce the Montreux document, the elitist nature of 'soft' regulations —a dominant characteristic of transnational governance— compounds the resulting democratic deficit. The UK's system confers the maximum freedom of action upon UK-based PMSCs operating abroad, while simultaneously undermining its own ability to command and control the use of force externally.[235] White argues that this self-regulation system for PMCs is inherently flawed because it is voluntary, has limited sanctions, and the standards agreed upon by and for the industry contain self-interested understandings of domestic and international laws.[236] These standards are neither national laws promulgated by a domestic legislature nor international laws created in inter-governmental fora; rather, they are described by the International Organization for Standards as the "distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent".[237] Ultimately the privatization of force is matched by the privatization of standards applicable to such force.

Case Study: International Code of Conduct (ICoC)

Initiative Emergence, Core Principles and Objectives

Growing dissatisfaction with the UN process, in conjunction with industry actors' articulation of a need for best practices —particularly in zones of weak governance where states were unable to uphold their obligations under the Montreux document— provided an impetus for pursuing regulation through a new

[234] Liu, *Law's Impunity*, 312.
[235] Nigel D. White, "Outsourcing Military and Security Functions," *AJIL Unbound* 115 (2021): 321, https://doi.org/10.1017/aju.2021.45.
[236] White, "Outsourcing Military," 321.
[237] White, "Outsourcing Military", 319.

institution. According to Prem, industry representatives conceived of the ICoC as an alternative to, and "competing with" the UN's ongoing initiatives, which they regarded as unduly biased against PMSCs.[238] Industry representatives solicited Switzerland for assistance in developing more practical (and putatively less biased) standards; Switzerland responded by orchestrating consultations with myriad stakeholders across government, civil society, industry, and academia in 2009. Although the notion of a corporate code was "essentially industry-driven",[239] the forum creation did not occur unilaterally: this initiative's multi-stakeholder character conferred upon it greater credibility, and PMSCs benefited from the support of numerous governments and NGOs.[240] The ICoC's stated objectives are to clarify international standards for "Member and Affiliate Companies… operating in complex… high risk, and fragile environments" while "act[ing] as a founding instrument… to create better governance, compliance, and accountability".[241] Its development adopted a two-stage process: following approval of the Code's final version occurring in 2010, the ICoC was operationalized through the Articles of Association for the International Code of Conduct Association (ICoCA) in 2013.[242] The ICoC incorporates a wide range of standards and principles for the responsible provision of security services, which can be summarized under two categories. Firstly, it includes principles regarding the conduct of Member Company personnel based on IHL and IHRL standards including rules on the use of force, human trafficking and child labor. Secondly, it articulates the appropriate management and governance of Member companies, including the selection, vetting, and training of personnel.[243, 244]

[238] Prem, "The Regulation," 357.
[239] Anne-Marie Buzatu, *Towards an International Code of Conduct for Private Security Providers: A View from inside a Multistakeholder Process*, 28, 2015, http://library.oapen.org/handle/20.500.12657/25839.
[240] Prem, "The Regulation," 358.
[241] International Code of Conduct Association, *International Code of Conduct for Private Security Service Providers*, Part A Art. 7, Part D Art. 13, December 10, 2021, https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF-CONDUCT_Amended_2021.pdf.
[242] Lubin, *Selling Surveillance,* 41.
[243] Maurer and Hoffmann, *The Privatisation*, 4.
[244] International Code of Conduct Association, *International Code*, Parts F and G.

Influence of Industry Actors

Although the UN Working Group process from which the MD emerged incorporated consultations with PMSCs, they remained embedded within a fundamentally state-centric framework. By contrast, the ICoC is distinctly appealing to PMSCs, raising them to equal partners in the regulatory process (as evident in the voting structure of the Board, the Association's primary decision-making body).[245,] Moreover, participation in the ICoC process has been largely limited to actors within civil society, industry, and government sharing the understanding that the PMSC industry should be permissively managed rather than entirely restricted.[246] This exclusivity of membership has allowed PMSCs to advance a policy agenda more closely aligned with their interests than the Draft Convention. By implication, the Code reflects the pro-privatization sentiments of industry stakeholders, and rather than taking issue with PMSCs, it instead attempts to transform them into more 'ethical' companies. Ultimately, although the ICoC implied subjecting the industry to a greater degree of scrutiny and constraints, in practice it has allowed PMSCs to retain greater authority over their fate. The fact that the ICoC was concluded largely by a consortium of PMSCs for the companies themselves means that it merely articulates principles for self-regulation, without a substantive legal effect.

The ICoC as a Normalizing & Legitimating Mechanism

Like the Montreux document, the ICoC performs a crucial legitimating function— yet it is arguably even more outspoken in its judgment of the industry's validity. Unlike the Montreux document, the ICoC also removes reference to the "military" attribute in describing these companies, and instead restricts the Code's applicatory scope to "security" contractors.[247] This discursive shift has transformed the legal debate, allowing PMSCs to dissociate themselves from proper military operations potentially reviving

[245] Buzatu, *Towards an International*, 55.
[246] Prem, "The Regulation," 358.
[247] International Code of Conduct Association, *International Code*, Preamble, Art. 1.

traditional images of mercenarism. This linguistic change is problematic because the Code's concern with "private security" contractors obfuscates the new activities in which PMSCs now engage— notably, military activities in cyberspace and the operation of drones, both of which carry the implication that PMSCs directly participate in hostilities.[248, 249] In this manner, the ICoC reaffirms PMSC's valid role in security governance, while the "military" category ceases to relevantly describe the industry. Signing the ICoC is a performative act insofar as it shifts the company's status from deviant to compliant, constructing the professional, socially responsible PMSC as a new kind of actor. Ultimately, the ICoC is concerned with establishing processes for reviewing compliance, rather than providing avenues of punishment and prevention for human rights abuses.[250] As a result, a PMSC's membership within the ICoC signals that it has established the necessary review and grievance procedures— yet crucially communicates nothing about its actual compliance with human rights in its operations. A problem arises where ICoC membership operates as a benchmark to guarantee the standard and quality of PMSCs, or functions as a prerequisite for awarding contracts (as the US and UK have proposed).[251]

The ICoC's Contractual Nature

The hierarchical organization of violence characterized by "effective control" is not only crucial to facilitate the flow of responsibility, but also critically structures preventative and remedial mechanisms aimed to promote compliance with international law. Implicit within the freedom of contract ideal is the notion that contractual parties are independent entities, equal in standing and status.[252] Whereas a state

[248] Chan, "The Need," 821.
[249] Berenike Prem, "The Regulation of Private Military and Security Companies: Analyzing Power in Multi-stakeholder Initiatives," *Contemporary Security Policy* 42, no. 3 (2021): Chap. 7.1, https://doi.org/10.1080/13523260.2021.1897225.
[250] Laura A. Dickinson, "Regulating the Privatized Security Industry: The Promise of Public/Private Governance," *Emory Law Journal* 63, no. 2 (2013): 429, https://scholarlycommons.law.emory.edu/elj/vol63/iss2/5?utm_source=scholarlycommons.law.emory.edu%2Felj%2Fvol63%2Fiss2%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages.
[251] Chan, "The Need," 822.
[252] Berndtsson and Kinsey, The Routledge, 138.

may still be regarded as allocating its monopoly on force through contracts with private actors, states lose their hierarchical position relative to PMSCs and are instead established as equals.[253] According to Liu, this dynamic has implications for state responsibility and attribution, because international law generally requires state action, authorization, or acquiescence to the act in question before ascribing responsibility to a state.[254] As a result, the horizontal nature of contractual relations subverts the operation of international legal mechanisms that depend upon the State occupying a position of command and control. For instance, consider the provision that "Signatory Companies will not, and will require that their Personnel do not, invoke *contractual obligations*, [or] superior orders… as a justification" for engaging in conduct proscribed by the ICoC.[255] This phrase effectively attempts to equate contractual obligations (arising from consensual agreement) with the defense of superior orders (expressing hierarchical relations characterized by effective control), highlighting a fundamental misunderstanding regarding contractual provisions' limitations in protecting human rights. The horizontal contractual relationship between a state and a PMSC enables the State to exert organized violence through the PMSC, while circumventing international responsibility and accountability frameworks reliant upon a hierarchical structure.

Self-Regulation and a Lack of Meaningful Accountability

Given the aforementioned two-stage process, companies that signed the ICoC (at least prior to the ICoCA's conclusion) endorsed the commitments embodied within the Code without awareness of their precise responsibilities under the actual accountability mechanism.[256] This suggests two cynical possibilities: firstly, that the companies believed that development of a rigorous mechanism was unlikely to occur, or secondly, that they would be able to dilute the salience of the enforcement mechanism

[253] Chan, "The Need," 823.
[254] Liu, *Law's Impunity*, 208.
[255] International Code of Conduct Association, *International Code*, Art. 23.
[256] This insight is based on the two-stage process characterizing the ICoC's development: whereas the Code's final version was approved in September 2010, the Articles of Association for the ICoCA (the ICoC's oversight institution) were not finalized until February 2013. See Seiberth, *Private Military*, 161-162.

through their participation in its development.[257] Unfortunately, normative commitments to the ICoC may substitute for genuine behavioral changes. The initial number of signatory companies was heavily inflated (708 PMSCs had signed in February 2013), reflecting merely symbolic adherence given the absence of initial barriers for determining corporate eligibility. [258] However, following the replacement of "signatory company" status in the Association to "transitional membership" requiring certification, the number declined to only 95 members.[259] This example highlights the performative dimension of the ICoCA distinction, particularly because the Association remains under-resourced, and many of its monitoring, reporting and grievance mechanisms have yet to be concretely implemented.[260]

Although the ICoC's efficacy critically depends upon the robustness of the "external independent mechanisms for effective governance and oversight" it called to establish,[261] these frameworks are hindered by the lack of transparency regarding the organization's processes, and of disciplinary measures available. The exclusive focus upon prospective responsibilities renders the ICoC "toothless and empty": lacking complementary accountability mechanisms, their fulfilment relies upon the ambiguities of "good faith".[262,263] Given the lack of specificity regarding *how* the ICoCA will monitor signatories' compliance to the ICoC, the danger remains that the ICoC will merely provide states with a fig-leaf to evade more rigorous, comprehensive efforts to regulate the industry, improve its standards, and ensure accountability for human rights and IHL. Absent significant, creative follow-up initiatives, the Document will at best remain a source of extensive doctrine and normative guidance— while lacking substantive implementation and enforcement arrangements.

---

[257] Liu, *Law's Impunity*, 313.
[258] Anna W. Chan, "The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber- Surveillance Spyware," *Brooklyn Journal of International Law* 44, no. 2 (2019): 820, https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/7.
[259] Prem, "The Regulation," 360.
[260] Boggero, *The Governance*, 86.
[261] International Code of Conduct Association, *International Code*, Art. 7.(b).
[262] International Code of Conduct Association, *International Code*, Art. 6.(f).
[263] Liu, *Law's Impunity*, 318.

Case Study: Wassenaar Arrangement (WA)

Initiative Emergence, Core Principles and Objectives

Unlike the preceding multi-stakeholder initiatives articulating the responsibilities of a particular public actor (state) or private actor (PMSC), the Wassenaar Arrangement focuses on restricting the export of the equipment, software, and expertise employed by companies in the military, security, and intelligence industry.[264] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) is a multilateral agreement between 42 member states aiming to promote transparency, consistency, and accountability in the proliferation of particular dual-use goods and technologies.[265] It emerged as the successor to the Coordination Committee for Multilateral Exports, a Cold War-era forum to mitigate the proliferation of sensitive technologies to the Soviet Union and Eastern Bloc.[266] The WA contains two core pillars: firstly, member states commit to maintaining a national export control over items on the WA control list, where decisions to allow for or deny export are the prerogative of each state (made "in accordance with national legislation and policies").[267] Secondly, the WA provides a forum for periodic meetings in Vienna, such that participating states can collectively discuss the implementation and consequences of various exports on their security needs.[268] It functions as a middle ground between uncoordinated national export policies, and a treaty imposing binding obligations to harmonize export controls. Because the "control list" of dual-use goods and technologies does not itself contain substantive treaty obligations, it has become common practice for both member states (like the US) and non-member states (such as China) to use this list as a reference point for developing and updating their domestic export control regimes.[269]

[264] Kim, "Global Export," 380.
[265] Broeders et al., *Artificial Intelligence*, 147.
[266] Riecke, "Unmasking the Term," 702.
[267] Fidler, "Regulating the Zero-Day," 702.
[268] Lubin, *Selling Surveillance*, 8.
[269] Kim, "Global Export," 380.

Following revelations that EU-based companies exported spyware to states that employed these technologies in violation of human rights during the Arab Spring, the United Kingdom and France (which had previously garnered criticism for their failure to prevent such exports) submitted proposals to restrict trade in several technologies.[270] Negotiations commenced among WA members regarding the addition of certain cyber-surveillance dual-use technologies (CSTs) to the WA control list.[271] The 2013 Cyber Amendments to the WA do not control the export of spyware *per se*, but rather, apply to "systems, equipment, and components… specifically designed or modified for the generation, command and control, or delivery of 'intrusion software' and technology for its development".[272] These Amendments have significantly impacted subsequent dual-use export reforms worldwide, particularly among the US, China, and the EU— who are leaders in the production, sales and governance of CSTs.[273] Whereas some updates to the WA are closely reflected in the creation of parallel mechanisms at the national level, the addition of CST's has proven more controversial.[274] CSTs constitute a test case examining the inability of conventional export control mechanisms to address myriad risks associated with the rapid technological development enabling the privatization of military and surveillance activities.

The Dual-Use Narrative and Commercial Interests

With regards to domestic implementation of internationally agreed-upon dual-use controls, the EU (European Union) has sought to enact the WA's Cyber Amendments under the EU Dual-Use Regulation.[275] This legal framework goes beyond the WA by explicitly categorizing CSTs as dual-use

[270] Riecke, "Unmasking the Term," 703.
[271] Lubin, *Selling Surveillance*, 10.
[272] Bureau of Industry and Security, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, report no. 2015-11642, May 20, 2015, https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.
[273] Innokenty Pyetranker, "An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement," *Northwestern Journal of Technology and Intellectual Property* 13, no. 2 (2015): 173-174, https://scholarlycommons.law.northwestern.edu/njtip/vol13/iss2/3.
[274] Kim, "Global Export," 380.
[275] Riecke, "Unmasking the Term," 700.

items. However, the EU's effort in codifying the WA demonstrates the consequences of employing export regulations to regulate a sphere of foreign policy with significant human rights implications. Consider the concept of "dual-use" underpinning the WA, which references a duality between an CST's perceived 'civil' and 'military' uses. This duality not only articulates the risks posed by cyber technologies and the rationale for controlling their export, but also *justifies* their trade. In particular, the term "dual use" may operate as a vehicle for commercial interests in the EU discourse regarding spyware export control. The European Commission has emphasized the military risks associated with dual-use items, while simultaneously depicting them as "cutting edge high-tech and… a reflection of the EU's technological leadership in the world".[276] By employing the 'civil' versus 'military' duality emerging from the "dual-use" narrative, the Commission rationalizes export control under state-centric security considerations (the potential for military application), while simultaneously endorsing the commercial exploitation of dual-use technologies' civil applications. These observations reflect the fact that dual-use export control policies were not traditionally intertwined with respect for human rights, but rather, developed to mitigate military risks in light of state-centric security and foreign policy interests.[277] Under these assumptions, civil applications of dual-use CSTs sold by PMSCs are necessarily legitimate and their trade need not be controlled. As highlighted in the first part of the analysis, the justifiability of exporting and importing CSTs, most notably spyware, is predicated on the human rights compliance of its end-uses— which ought to be assessed rather than assumed. By instrumentalizing the duality generated by the term "dual use", governments have advanced the assumption that dual-use items necessarily have a use for which trade is reasonable, to legitimize ongoing trade in CSTs used in contemporary warfare.

[276] Fidler, "Regulating the Zero-Day," 469.
[277] Riecke, "Unmasking the Term," 708.

Domestic Implementation and Enforcement Challenges

Despite its Cyber Amendments designed to control surveillance technologies, the WA has encountered significant enactment and enforcement challenges, manifest as discrepancies in the extent to which various major states have incorporated the WA's principles within their domestic legislation. Although implementation of this soft-law mechanism crucially depends on national discretion, governments remain hesitant to regulate software they use or to penalize the companies developing it within their borders.[278] For instance, in 2015, the U.S. Commerce Department issued a proposal, modelled on Wassenaar, which would have introduced additional licensing requirements to export "intrusion software" of the sort sold by HT, Gamma Group, and other vendors,. This proposal garnered criticism for its propensity to "detrimentally affect [American] national security" and "completely [destroy] vulnerability research… slowing the disclosure of vulnerabilities and impairing [the] nation's cybersecurity".[279] However, it is virtually impossible to discriminate between companies developing and testing vulnerability-probing software, and those endeavoring to create zero-day exploits and intrusion capabilities.[280] This example demonstrates how the US and private technology companies have actively sought to limit the scope of the WA's export controls, fearing overly-broad controls limiting researchers' capacity to identify security vulnerabilities, and criminalizing crucial tools for stopping malware. Ultimately, the technologies the WA seeks to control have become so pervasive that oversight is nearly impossible, and further regulatory attempts could drive the markets for such products deeper underground.

[278] Lubin, *Selling Surveillance,* 11.
[279] Burkart and McCourt, "The International," 49.
[280] Burkart and McCourt, "The International," 51.

Comparative Analysis of Multi-Stakeholder Initiatives

I. Participation and Enforcement Challenges

A rift in regulatory models has emerged between more stringent, robust legal frameworks regulating privatized warfare (the Draft Convention), and soft law mechanisms (the MD, ICoC, and the WA). The Draft Convention has confronted issues of legitimacy, capacity, and political commitment, undermining its adoption in the face of two competing initiatives, the Montreux Document and the ICoC. This challenge is reflected in the US' failure to domestically implement the comprehensive monitoring and redress protocols outlined within the Draft Convention, despite possessing the capacity to do so. Because the MD and the ICoC are endorsed by powerful states profoundly engaged with PMSCs, their ongoing participation in these soft-law processes would undermine the Draft Convention's relevance and legitimacy, if it is ever enacted. Despite the reaffirmation of binding IHL and IHRL norms within the MD and the ICoC, the failure to establish (and realize) concomitant oversight mechanisms undermines the possibility of these initiatives giving their own norms autonomous, binding force. As described in the case study, the ICoC's efficacy critically depends upon the external independent oversight Association it purports to establish. However, the lack of specificity regarding this institution's functioning suggests that ICoC membership may merely offer superficial legitimacy for companies seeking to evade more rigorous, comprehensive regulatory efforts.

Moreover, because international law is formulated by states for states, domestic regulation remains paramount to international law's effective implementation, and the crystallization of new international norms regarding PMSCs. Invoking Hurd's notion of law as both permissive and empowering, the failure of international law to address warfare's privatization is exacerbated by states' *choice* to not subject themselves to international standards in favor of soft laws or the promotion of corporate self-regulation. The bypassing is logical, because existing law does not establish sufficiently specific conceptual and policy guidelines, and extends neither penalties for violation nor incentives for compliance. In the context

of the MD implementation, the United Kingdom —an actor strongly endorsing the Document's creation— disregarded the provision recommending that home States establish authorization systems. Instead, the United Kingdom opted for a system with standards developed by and for the PMSC industry, affording these companies maximum freedom of action.

Finally, the market for private military and spyware capabilities remains a lucrative business; corporate money translates to power and influence over decision-makers who would consider constraints on the industry. As a result, governments are often reluctant to take the necessary measures to regulate these actors and their services. As illustrated by the WA case study, domestic constituencies frequently take advantage of opportunities to challenge, dilute, or evade norms formally agreed upon at the international level. An export control mechanism designed to regulate trade in CSTs, the WA's ability to address human rights concerns resulting from their trade has been undermined by countries' desire to pursue vulnerability research and other commercial interests. Despite the importance of regulatory consistency and harmonization across jurisdictions application of export control regimes, concerns of maintaining an advantage in technological development over strategic competitors has contributed to divergent (and overly permissive) measures regarding the trade of CSTs employed by PMSCs.

II. The Performative and Normalizing Dimensions of Regulatory Initiatives

From a cynical perspective, one may argue that the very attractiveness of voluntary self-regulatory regimes (such as the MD and the ICoC) is that the members enjoy an advantage relative to the regulatory body, and derive a range of benefits from membership with minimal associated costs. Moreover, a tension exists when considering a self-regulatory body's reputation: it must uphold the impression that it can effectively monitor industry actors in the public's interest, while maintaining the perception among

industry actors that it operates in their favor.[281] The proliferation of voluntary standards has enforced PMSC's entrenchment in contemporary security matters, by legitimizing new spheres of activity for the industry. From an institutional perspective, these initiatives signify a transition away from binding international regulation through the UN, the ICRC, and other intergovernmental bodies towards decentralized, self-regulatory frameworks that serve the neoliberal agendas of Western governments and like-minded actors in industry.

The analysis of the MD noted that this framework defines military and security functions extremely broadly, in order to secure endorsement from influential states with permissive security outsourcing cultures. The neutral label selected to describe commercial military and security providers as "PMSCs" substantiates these actors' own efforts to distance themselves from the negative connotations accompanying the concepts of "mercenary" and "combatant". By beginning from the assumption PMSCs ought to be regulated permissively rather than criminalized, the MD helps to normalize the practice of privatized security. Furthermore, examining the MD's provisions also foregrounds the shortcomings of contractually-based remedies for human rights violations, by demonstrating their propensity to dilute fundamental IHL and IHRL principles. The ICoC's transformative dialogue serves a performative function insofar as it insinuates subjecting the industry to greater scrutiny and restrictions— yet in practice, has empowered them to retain greater control over their fate. In particular, the horizontal nature of the contractual relationship between a state and a private company relegates the position of the state, frustrating attempts to impute responsibility and accountability under the "effective control" principle of international law. Membership within the ICoC also constitutes a performative act, by allowing a PMSC to distinguish itself as "compliant" and "socially responsible". It signals that the company has established the requisite review and redress mechanisms, without communicating substantive information regarding its actual human rights compliance during operations. Furthermore, by restricting the Code's applicatory

[281] Liu, *Law's Impunity,* 324.

scope to "security" contractors and removing references to the "military" attribute in describing the industry, the ICoC has transformed the legal debate, by implying that only security contractors are problematic and require regulation. Both the MD and the ICoC privilege and reinforce the perspectives of those actors sharing the belief that PMSCs should be permissively regulated rather than entirely banned. The concept of "good governance" of the PMSC industry is foundational to the discourses and practices emerging from these two MSIs, where the rules intended to govern PMSCs have erased earlier, negative representations of PMSCs.

Finally, analyzing the WA revealed the definitional power of "dual-use" capabilities to normalize trade in the technologies used by PMSCs, by emphasizing their unproblematic nature insofar as they remain used for "civil" rather than "military" purposes. The WA's status as an export control framework is ill-suited to addressing the contextual ambiguities inherent in these technologies' employment by PMSCs. Within domestic regulation, the WA's provisions are often instrumentalized to promote state-centric commercial interests regarding these technologies' trade, while overlooking human-centric human rights concerns emanating from their use.

III. International Regulatory Initiatives and Inequality

Despite the laudable intentions and some substantial benefits of juridifying the use of force, this process can marginalize competing paradigms and become myopic. As previously discussed, the international law regulating conflict and security matters is created, interpreted, and (selectively) enforced by powerful actors in government and industry to advance their own interests. Legal institutions, despite their claim to objectivity and neutrality, remain vulnerable "to capture by states, by ideologies, [and] by other agendas".[282] For instance, viewing the Draft Convention's provisions as unacceptable (particularly its narrow definition of "inherent state functions" prohibiting the outsourcing of a wide range of functions),

[282] Liu, *Law's Impunity,* 26.

the US and the UK repeatedly attempted to obstruct the UN Working Group's activities through *forum blocking*. Subsequently, they pursued *forum shifting* by endorsing the Swiss Initiative (from which the MD emerged), and the ICoC. These multilateral initiatives have allowed Western governments and the PMSC industry to circumvent alternative avenues for corporate regulation, notably the hard-law UN Draft Convention, which represented the perspective of states more skeptical of these entities.

In juxtaposition with the more inclusive environment characterizing the Draft Convention process, participation in the MD and the ICoC has been limited to groups holding a favorable attitude toward PMSCs. As demonstrated in the MD case study, non-governmental actors were excluded from the final stages of negotiation, while influential governments took advantage of the chance to dilute the Convention's provisions to reflect their interests. The marginalization of critical voices as inferior forms of expertise has rendered it possible to present hybrid public-private rules through multi-stakeholder contracts as though they are the only regulatory option available, even though alternative mechanisms have been considered within the international community. Moreover, the exclusivity of membership characterizing the ICoC renders it a reflection of the privatization-friendly sentiments of industry stakeholders. In the case of the WA, the US' dominant position as a producer and consumer of spyware and intelligence technologies disincentivizes market regulation, and encourages international trade in code entities (such as zero-day exploits). This dynamic has undermined the development of an effective governance architecture for regulating and prohibiting technologies used by PMSCs in offensive cyber operations.

IV. Balancing Apology and Utopia in the Regulation of Privatized Security

The Draft Convention, Montreux Document, ICoC and WA constitute prima facie evidence of emerging norms on PMSCs, but whether these initiatives are meaningfully contributing to an evolving legal and political discourse on PMSCs (and to the formation of new norms) remains an open question. Drawing on

Koskenniemian themes explored in the literature review, it remains unclear how the MD and the ICoC — as concrete, pragmatic responses to political realities— can establish a middle ground between apologizing for state power and other hegemonic interests, and articulating norms the international community may consider unrealistic and irrelevant.

The Draft Convention represents "utopia" in the sense that its provisions, although theoretically admirable, are too idealistic to garner widespread endorsement among influential states. It provides for strong international accountability, transparency, and due diligence mechanisms, complemented by articles requiring States Parties to enact specific enforcement frameworks domestically. However, despite garnering support from Russia, China, and most developing countries, the Convention was met with resistance from industry representatives, and prolific PMSC users (the UK, the US, and the EU). By contrast, the MD, ICoC and WA constitute "apologies" for state power. To garner the support of the US and UK, the MD contains a much more expansive understanding of the state functions transferrable to private actors than the Draft Convention. Analyzing the linguistic amendments gradually introduced during the MD negotiation process highlighted numerous caveats regarding the extent of states' treaty and customary obligations, and emphasized the Document's non-binding nature. Whereas the MD's soft-law approach recalls (and arguably dilutes) existing legal obligations under IHL and IHRL, the ICoC takes an even softer approach, advocating principle norms under an industry-oriented code of conduct. Moreover, the WA apologizes for government's commercial interests by legitimizing CST's 'civil' uses, while marginalizing the human rights considerations associated with PMSC's employment of these technologies. The MD, ICoC and WA exhibit concreteness in the sense that they have garnered widespread support from key participants within the market for force. Yet as a corollary to accurately reflecting the facts of international politics, these initiatives are shaped to advance the opinions and objectives of influential actors in government and industry. Taken together, the case studies illustrate the challenge international laws and norms face in remaining sufficiently precise to remain relevant, yet sufficiently ambiguous that they will receive endorsement among a critical mass of states.

This section of the Analysis explored how the Draft Convention, MD, ICoC, and WA adopt diverse regulatory approaches expressing commitments to understand applicable international laws, developing normative standards, and implementing accountability measures regarding PMSCs and the technologies they employ. Contextualizing each initiative in terms of the conditions leading to its emergence and its espoused objectives allowed for a subsequent exploration of the negotiation, revision, and implementation of provisions among the actors involved.

Conclusion

Revisiting the Research Question

The question motivating this inquiry is as follows:

To what extent have multilateral initiatives effectively addressed the practical, legal and normative challenges presented by the increasing legitimacy and influence of private actors in contemporary conflicts?

Combining the findings from Part B with insights from Part A exhibits how these multilateral frameworks often only provide the semblance of meaningful regulation and clarification, and ultimately reproduce many of the same challenges they purport to address.

An answer to the research question incorporating both sections of the analysis is provided below:

- As described in Part A, PMSCs have consolidated their legitimacy by invoking their status as security and risk experts, by emphasizing their efficiency as private actors in a neoliberal ideological climate, and by providing a range of non-combat services to dissociate themselves from the controversial

"mercenary" label. This dynamic resurfaces in Part B: the authority these companies enjoy has allowed them to initiate self-regulatory efforts including the ICoC, while the Montreux Document legitimizes the industry by removing references to mercenarism, and conceptualizing PMSCs as a distinct phenomenon.

- Moreover, Part A described how governments have actively created and sustained demand for PMSCs, benefiting from the plausible deniability these proxy actors provide despite the disadvantages of reduced sovereign control in conflict situations. In reflection of this demand, major global powers, as prolific PMSC users, have disproportionately influenced the debate regarding these companies' regulation. As described in Part B, by engaging in forum blocking (of the Draft Convention), and forum transformation (endorsing the MD), they have effectively advanced their perspectives within their preferred international fora. This dynamic has had the effect of marginalizing the criticisms of less powerful states and non-governmental actors presenting opposing insights.
- Furthermore, Part A considered the challenges of applying existing international laws to these new categories of private actors. Analyzing the language of provisions within the MD and ICoC in Part B (which purport to clarify IHL and IHRL principles relevant to PMSCs) reveals that these provisions remain fraught with definitional ambiguities. Part B also revealed how the MD's and ICoC's contractual structures have the propensity to dilute existing international laws, while elevating the status of PMSC actors to equal standing with states. As a result, these initiatives normalize and legitimate PMSCs as international security providers.
- Evaluating the interplay between privatization and technological development, Part A argued that the extension of PMSC's capabilities to the cyber and intelligence realms exacerbates the accountability and attribution challenges inherent in "traditional" PMSC regulation. This section also acknowledged the difficulty of regulating trade in the "dual-use" technologies employed by PMSCs in a globalized world, particularly when these actors operate clandestinely and cross-jurisdictionally. By analyzing the WA, Part B problematized its definition of "dual-use" technologies: rather than limiting the trade

of CSTs given their potential for offensive use by PMSCs, this export control regime serves states' commercial interests by justifying their trade.

- Finally, the ease with which states can evade legal responsibility by employing PMSCs as proxies, as described in Part A, is reproduced by the fact that they can selectively enforce the voluntary arrangements described in Part B to serve their economic and political interests. Practical realities regarding relatively weak implementation procedures (even among states possessing the capacity to enforce internationally agreed-upon frameworks) has undermined the crystallization of these norms and laws on the domestic level.

Limitations and Directions for Future Research

One significant methodological limitation of this research concerns the difficulty of accessing accurate, comprehensive information regarding particular actors within the PMSC industry in light of time and resource constraints. The selected examples and events corroborating the insights regarding the challenges posed by PMSCs were verified through multiple primary and secondary sources to ensure a degree of objectivity and unbiasedness. However, future research in this discipline could draw examples from a more comprehensive subset of PMSCs, and seek more information from primary sources regarding these entities (particularly through first-hand interviews of security experts, government officials, or PMSC employees).

Moreover, the content limitations of this project highlight two promising avenues for future research. Firstly, one could pivot from exploring the interaction between privatization and technological development (as it pertains to the cyber and intelligence fields), to instead explore the implications of automation as it pertains to private contractor capabilities. This would entail a fusion of the literature regarding autonomous weapons systems (AWS) and of the legal and normative implications of privatizing warfare. Secondly, in focusing primarily upon macro-level international initiatives and the behaviors of several PMSCs, this inquiry neglected to explore the extent to which civil society actors

have drawn attention to the accountability challenges posed by PMSCs, and incentivized regulatory initiatives. Additional research could analyze the role of NGOs, journalists, and media organizations in illuminating and interrogating the outsourcing of warfare to corporate entities.

In conclusion, this analysis has not only offered a comparative case study of international society's attempts to understand and regulate PMSCs in light of the challenges that technologically advanced, privatized conflict poses to existing legal frameworks; it also exemplifies how the terrain of international law remains entangled in the subjectivities of international politics. Implementable laws and norms must navigate a compromise between reflecting the concrete realities and the interests of the powerful, and still articulating meaningful, countervailing normative principles. The evidence explored in this paper suggests that states are failing to socially, politically, and legally internalize norms regarding the regulation of contemporary privatized, technologically advanced warfare. In this context, international law's intellectual and moral validity appears to have weakened, such that it merely constrains the superficial appearance of actors' behavior, rather than their substantive actions. Nevertheless, the international legal system retains value as a framework through which new norms and principles may be articulated, debated, and potentially adopted within the international community in the future. Although prone to instrumentalist invocation, the law's malleability confers upon it a remarkable resilience. International law offers a forum for actors from diverse backgrounds to claim responsibility for the law's evolution. By engaging with, contesting, and redefining shared principles, states, companies, and civil society actors can envision a collective future of more ethical conflict, despite the fundamental challenges posed by the contemporary privatization of war.

Bibliography

Al Aridi, Alaa Al Dakour. "The Problem of Hybrid Warfare in International Law." PhD diss., Vilnius University, 2022.

Alexander, Atul, and Tushar Krishna. "Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism." *Laws* 11, no. 6 (2022): 85. https://doi.org/10.3390/laws11060085.

Allenby, Braden R. "Are New Technologies Undermining the Laws of War?" *Bulletin of the Atomic Scientists* 70, no. 1 (2014): 21-31. https://doi.org/10.1177/0096340213516741.

Amnesty International. *Amnesty International Public Statement on the Montreux Document*. October 14, 2008. https://www.amnesty.org/en/wp-content/uploads/2021/07/ior300102008en.pdf.

Aust, Helmut Philipp. "Hybrid Warfare and the Turn to Resilience: Back to the Cold War?" *Humanitäres Völkerrecht* 3, nos. 3-4 (2020): 293-310. https://doi.org/10.35998/huv-2020-0017.

Avant, Deborah. "The Privatization of Security and Change in the Control of Force." *International Studies Perspectives* 5, no. 2 (2004): 153-57. https://doi.org/10.1111/j.1528-3577.2004.00165.x.

Avant, Deborah D. "Pragmatic Networks and Transnational Governance of Private Military and Security Services." *International Studies Quarterly* 60, no. 2 (2016): 330-42. https://doi.org/10.1093/isq/sqv018.

Bachmann, Sascha-Dominik, and Håkan Gunneriusson. "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security." *Scientia Militaria: South African Journal of Military Studies* 43, no. 1 (2015): 77-98. https://doi.org/10.5787/43-1-1110.

Balcaen, Pieter, Cind Du Bois, and Caroline Buts. "A Game-theoretic Analysis of Hybrid Threats." *Defence and Peace Economics* 33, no. 1 (2021): 26-41. https://doi.org/10.1080/10242694.2021.1875289.

Bergman, Ronen, and Mark Mazzetti. "The Battle for the World's Most Powerful Cyberweapon." *The New York Times*, January 28, 2022. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

Berndtsson, Joakim, and Christopher Kinsey. *The Routledge Research Companion to Security Outsourcing*. New York, NY: Routledge, Taylor & Francis Group, 2016.

Bode, Ingvild, and Hendrik Huelss. *Autonomous Weapons Systems and International Norms*. Montreal, QC: McGill-Queen's University Press, 2022.

Boggero, Marco. *The Governance of Private Security*. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-69593-8.

Broeders, Dennis, Fabio Cristiano, François Delerue, Frédérick Douzet, and Aude Géry. *Artificial Intelligence and International Conflict in Cyberspace*. New York, NY: Routledge, 2023. https://doi.org/10.4324/9781003284093.

Bureau of Industry and Security. *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*. Report no. 2015-11642. May 20, 2015. https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

Burkart, Patrick, and Tom McCourt. "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software." *Popular Communication* 15, no. 1 (2017): 37-54. https://doi.org/10.1080/15405702.2016.1269910.

Buzatu, Anne-Marie. *Towards an International Code of Conduct for Private Security Providers: A View from inside a Multistakeholder Process*. 2015. http://library.oapen.org/handle/20.500.12657/25839.

Calcara, Antonio. "Contractors or Robots? Future Warfare between Privatization and Automation." *Small Wars and Insurgencies* 33, nos. 1-2 (2021): 250-71. https://doi.org/10.1080/09592318.2021.1957534.

Carpanelli, Elena, and Nicole Lazzerini, eds. *Use and Misuse of New Technologies*. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-05648-3.

Chan, Anna W. "The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber- Surveillance Spyware." *Brooklyn Journal of International Law* 44, no. 2 (2019): 795-830. https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/7.

Chesterman, S. "We Can't Spy ... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions." *European Journal of International Law* 19, no. 5 (2008): 1055-74. https://doi.org/10.1093/ejil/chn055.

Cockayne, James. "Private Military and Security Companies." *The Oxford Handbook of International Law in Armed Conflict*, June 2, 2014, 624-55. https://doi.org/10.1093/law/9780199559695.003.0025.

Cockayne, James. "Regulating Private Military and Security Companies: The Content, Negotiation, Weaknesses and Promise of the Montreux Document." *Journal of Conflict and Security Law* 13, no. 3 (2008): 401-28. https://doi.org/10.1093/jcsl/krp006.

Cody, Stephen. "Dark Law: Legalistic Autocrats, Judicial Deference, and the Global Transformation of National Security." *University of Pennsylvania Journal of Law & Public Affairs* 6, no. 4 (2021): 643-86. https://scholarship.law.upenn.edu/jlpa/vol6/iss4/2.

Cole, Matthew. "The Complete Mercenary." *The Intercept*, May 3, 2019. https://theintercept.com/2019/05/03/erik-prince-trump-uae-project-veritas/.

Connolly, Daniel. "New Rules for New Tools? Exploitative and Productive Lawfare in the Case of Unpiloted Aircraft." *Alternatives: Global, Local, Political* 43, no. 3 (2018): 137-56. https://doi.org/10.1177/0304375419835039.

Cusumano, Eugenio. *Mobilization Constraints and Military Privatization*. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-16423-1.

Cusumano, Eugenio "Policy Prospects for Regulating Private Military and Security Companies." *War by Contract*, January 1, 2011, 11-36. https://doi.org/10.1093/acprof:oso/9780199604555.003.0002.

Cusumano, Eugenio, and Christopher Kinsey. "Concluding Comments." *Small Wars and Insurgencies* 33, nos. 1-2 (2021): 294-312. https://doi.org/10.1080/09592318.2022.2021487.

Cutler, A. C. "The Legitimacy of Private Transnational Governance: Experts and the Transnational Market for Force." *Socio-Economic Review* 8, no. 1 (2009): 157-85. https://doi.org/10.1093/ser/mwp027.

de Groot, Tom, and Salvador Santino F Regilme. "Private Military and Security Companies and the Militarization of Humanitarianism." *Journal of Developing Societies* 38, no. 1 (2021): 50-80. https://doi.org/10.1177/0169796x211066874.

Dickinson, Laura A. "Contractors and Hybrid Warfare: A Pluralist Approach to Reforming the Law of State Responsibility." In *States, Firms, and Their Legal Fictions*, edited by Melissa J. Durkee, 69-86. Cambridge University Press, 2024. https://doi.org/10.1017/9781009334709.005.

Dickinson, Laura A. "Regulating the Privatized Security Industry: The Promise of Public/Private Governance." *Emory Law Journal* 63, no. 2 (2013): 417-54. https://scholarlycommons.law.emory.edu/elj/vol63/iss2/5?utm_source=scholarlycommons.law.emory.edu%2Felj%2Fvol63%2Fiss2%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages.

Dingwerth, Klaus, and Philipp Pattberg. "World Politics and Organizational Fields: The Case of Transnational Sustainability Governance." *European Journal of International Relations* 15, no. 4 (2009): 707-43. https://doi.org/10.1177/1354066109345056.

Fidler, Mailyn. "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis." *I/S: A Journal of Law and Policy for the Information Society* 11, no. 2 (2015): 405-83. https://ssrn.com/abstract=2706199.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887-917. https://doi.org/10.1162/002081898550789.

Fogt, Morten M. "Legal Challenges or 'Gaps' by Countering Hybrid Warfare - Building Resilience in Jus Ante Bellum." *Southwestern Journal of International Law* 27, no. 1 (2021): 29-100. https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf.

G4S. *Intelligence and Advisory Services (IAS) Capability*. https://www.g4sriskmanagement.com/-/media/g4s/riskmanagement/indexed-files/files/ias_protea_capability_-_final__-5_may.ashx?la=en&hash=385DA8129A45978CAF8A5B7195CEF19E.

Gasser, Martina, and Mareva Malzacher. "Beyond Banning Mercenaries: The Use of Private Military and Security Companies under IHL." In *International Humanitarian Law and Non-State Actors: Debates, Law and Practice*, edited by Ezequiel Heffes, Marcos D. Kotlik, and Manuel J. Ventura, 47-77. The Hague: T.M.C. Asser Press, 2020. https://doi.org/10.1007/978-94-6265-339-9_3.

Gerring, John. "The Case Study: What It Is and What It Does." *The Oxford Handbook of Comparative Politics*, September 2, 2009, 90-122. https://doi.org/10.1093/oxfordhb/9780199566020.003.0004.

Hakimi, Monica. "The Work of International Law." *Harvard International Law Journal* 58, no. 1 (2017): 1-46.

Hathaway, Oona, and Scott J. Shapiro. "Outcasting: Enforcement in Domestic and International Law." *Yale Law Journal* 121, no. 2 (2011): 252-349.

Hurd, Ian. "The International Rule of Law and the Domestic Analogy." *Global Constitutionalism* 4, no. 3 (2015): 365-95. https://doi.org/10.1017/s2045381715000131.

Huskey, Kristine A. "Accountability for Private Military and Security Contractors in the International Legal Regime." *Criminal Justice Ethics* 31, no. 3 (2012): 193-212. https://doi.org/10.1080/0731129x.2012.737169.

International Code of Conduct Association. *International Code of Conduct for Private Security Service Providers*. December 10, 2021. https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF-CONDUCT_Amended_2021.pdf.

International Committee of the Red Cross, and Swiss Federal Department of Foreign Affairs. *The Montreux Document*. August 2009. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf.

International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. 2001. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

Kaldor, Mary. *New and Old Wars: Organized Violence in a Global Era*. 2nd ed. Cambridge: Polity, 2010.

Kaster, Sean D., and Prescott C. Ensign. "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware." *Thunderbird International Business Review* 65, no. 3 (2022): 355-64. https://doi.org/10.1002/tie.22321.

Kim, Heejin. "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue." *International and Comparative Law Quarterly* 70, no. 2 (2021): 379-415. https://doi.org/10.1017/s0020589321000105.

Kinsella, Helen M., and Giovanni Mantilla. "Contestation before Compliance: History, Politics, and Power in International Humanitarian Law." *International Studies Quarterly* 64, no. 3 (2020): 649-56. https://doi.org/10.1093/isq/sqaa032.

Kittrie, Orde F. *Lawfare: Law as a Weapon of War*. Oxford: Oxford University Press, 2016.

Koskenniemi, Martti. *From Apology to Utopia: The Structure of International Legal Argument*. Cambridge: Cambridge University Press, 2015.

Krahmann, Elke. "The United States, PMSCs and the State Monopoly on Violence: Leading the Way towards Norm Change." *Security Dialogue* 44, no. 1 (2013): 53-71. https://doi.org/10.1177/0967010612470292.

Krahmann, Elke. "From Performance to Performativity: The Legitimization of US Security Contracting and Its Consequences." *Security Dialogue* 48, no. 6 (2017): 541-59. https://doi.org/10.1177/0967010617722650.

Krahmann, Elke. "From 'Mercenaries' to 'Private Security Contractors': The (Re)Construction of Armed Security Providers in International Legal Discourses." *Millennium: Journal of International Studies* 40, no. 2 (2011): 343-63. https://doi.org/10.1177/0305829811426673.

Krieg, Andreas. "The UAE's 'Dogs of War': Boosting a Small State's Regional Power Projection." *Small Wars & Insurgencies* 33, nos. 1-2 (2021): 152-72. https://doi.org/10.1080/09592318.2021.1951432.

Krieg, Andreas, and Jean-Marc Rickli. *Surrogate Warfare: The Transformation of War in the Twenty-First Century*. Washington, DC: Georgetown University Press, 2019.

Kruck, Andreas. "Theorising the Use of Private Military and Security Companies: A Synthetic Perspective." *Journal of International Relations and Development* 17, no. 1 (2013): 112-41. https://doi.org/10.1057/jird.2013.4.

Kushner, David. "Fear This Man." *Foreign Policy*, April 26, 2016. https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/.

Leander, Anna. *Eroding State Authority? Private Military Companies and the Legitimate Use of Force*. 2006. https://www.files.ethz.ch/isn/20511/Eroding_State_authority.pdf.

Leander, Anna. "The Paradoxical Impunity of Private Military Companies: Authority and the Limits to Legal Accountability." *Security Dialogue* 41, no. 5 (2010): 467-90. https://doi.org/10.1177/0967010610382108.

Leander, Anna. "The Power to Construct International Security: On the Significance of Private Military Companies." *Millennium: Journal of International Studies* 33, no. 3 (2005): 803-25. https://doi.org/10.1177/03058298050330030601.

Liu, Hin-Yan. *Law's Impunity: Responsibility and the Modern Private Military Company*. Oxford, United Kingdom: Hart Publishing, 2017.

Lost, Jack. "In Central Africa, Russia Won the War—but It's Losing the Peace." *Foreign Policy*, August 21, 2021. https://foreignpolicy.com/2021/08/21/in-central-africa-russia-won-the-war-but-its-losing-the-peace/.

Lubin, Asaf. *Selling Surveillance*. Research report no. 495. 2023. https://ssrn.com/abstract=4323985.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge, United Kingdom: Cambridge University Press, 2018.

Maurer, Tim, and Wyatt Hoffmann. *The Privatisation of Security and the Market for Cyber Tools and Services*. July 2019. https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf.

McFate, Sean. *The Modern Mercenary: Private Armies and What They Mean for World Order*. Oxford, United Kingdom: Oxford University Press, 2017.

Michaels, Jon D. "Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War." *Washington University Law Review* 82, no. 3 (2004): 1001-127. https://openscholarship.wustl.edu/law_lawreview/vol82/iss3/6.

Monoghan, Sean. "Countering Hybrid Warfare So What for the Future Joint Force?" *PRISM* 8, no. 2 (2019): 82-98. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf.

Morse, Julia C., and Robert O. Keohane. "Contested Multilateralism." *The Review of International Organizations* 9, no. 4 (2014): 385-412. https://doi.org/10.1007/s11558-014-9188-2.

Mumford, Andrew. "Proxy Warfare and the Future of Conflict." *The RUSI Journal* 158, no. 2 (2013): 40-46. https://doi.org/10.1080/03071847.2013.787733.

Münkler, Herfried. *The New Wars*. Cambridge, UK: Polity, 2005.

Østensen, Åse Gilje, and Tor Bukkvoll. "Private Military Companies – Russian Great Power Politics on the Cheap?" *Small Wars and Insurgencies* 33, nos. 1-2 (2021): 130-51. https://doi.org/10.1080/09592318.2021.1984709.

Papademetriou, George T. "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry." *Harvard Human Rights Journal*

36, no. 2 (2023): 191-221. https://journals.law.harvard.edu/hrj/wp-content/uploads/sites/83/2023/06/HLH105_crop.pdf.

Pattison, James. "The Challenge of PMSCs." *The Morality of Private War*, May 29, 2014, 1-25. https://doi.org/10.1093/acprof:oso/9780199639700.003.0001.

Percy, Sarah V. "Mercenaries: Strong Norm, Weak Law." *International Organization* 61, no. 02 (2007). https://doi.org/10.1017/s0020818307070130.

Perlroth, Nicole, and David E. Sanger. "Nations Buying as Hackers Sell Flaws in Computer Code." *The New York Times* (New York, NY), July 13, 2013. https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

Petersohn, Ulrich. "Reframing the Anti-mercenary Norm: Private Military and Security Companies and Mercenarism." *International Journal: Canada's Journal of Global Policy Analysis* 69, no. 4 (2014): 475-93. https://doi.org/10.1177/0020702014544915.

Pils, Eva. "Autocratic Challenges to International Human Rights Law: A Chinese Case Study." *Current Legal Problems* 75, no. 1 (2022): 189-236. https://doi.org/10.1093/clp/cuac007.

Prem, Berenike. "Who Am I? The Blurring of the Private Military and Security Company (PMSC) Category." *Security Privatization*, July 4, 2017, 51-76. https://doi.org/10.1007/978-3-319-63010-6_3.

Prem, Berenike. *Private Military and Security Companies as Legitimate Governors: From Barricades to Boardrooms*. London, United Kingdom: Routledge, 2020.

Prem, Berenike. "The Regulation of Private Military and Security Companies: Analyzing Power in Multi-stakeholder Initiatives." *Contemporary Security Policy* 42, no. 3 (2021): 345-70. https://doi.org/10.1080/13523260.2021.1897225.

Pyetranker, Innokenty. "An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement." *Northwestern Journal of Technology and Intellectual Property* 13, no. 2 (2015): 153-80. https://scholarlycommons.law.northwestern.edu/njtip/vol13/iss2/3.

Rauta, Vladimir. "Towards a Typology of Non-state Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces." *Cambridge Review of International Affairs* 33, no. 6 (2019): 868-87. https://doi.org/10.1080/09557571.2019.1656600.

Riecke, Lena. "Unmasking the Term 'Dual Use' in EU Spyware Export Control." *European Journal of International Law* 34, no. 3 (2023): 697-720. https://doi.org/10.1093/ejil/chad039.

Sari, Aurel. "Hybrid Warfare, Law, and the Fulda Gap." In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, edited by Winston S. Williams and Christopher M. Ford, 161-90. Oxford University Press, 2018. https://doi.org/10.1093/oso/9780190915360.003.0006.

Seiberth, Corinna. *Private Military and Security Companies in International Law: A Challenge for Non-binding Norms: The Montreux Document and the International Code of Conduct for Private Security Providers*. Cambridge, UK: Intersentia, 2014.

Simmons, Beth A. "Why International Law? The Development of the Human Rights Regime in the Twentieth Century." In *Mobilizing for Human Rights: International Law in Domestic Politics*, 23-56. Cambridge University Press, 2009. https://doi.org/10.1017/CBO9780511811340.002.

Singer, P.W. *Corporate Warriors: The Rise of the Privatized Military Industry*. 2nd ed. Ithaca, N.Y.: Cornell University Press, 2008.

Singer, P.W. "Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security." *International Security* 26, no. 3 (2002): 186-220. https://doi.org/10.1162/016228801753399763.

Sorensen, Kim. "The Politics of International Law: The Life Cycle of Emerging Norms on the Use and Regulation of Private Military and Security Companies." *Griffith Law Review* 26, no. 1 (2017): 89-127. https://doi.org/10.1080/10383441.2017.1339773.

Swed, Ori, and Daniel Burland. "Outsourcing War and Security." In *Oxford Research Encyclopedia of Politics*. Oxford University Press, 2020. https://doi.org/10.1093/acrefore/9780190228637.013.1925.

Swed, Ori, and Thomas Crosbie, eds. *The Sociology of Privatized Security*. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-98222-9.

Taylor, Trevor. "Contractors on Deployed Operations and Equipment Support." *Defence Studies* 4, no. 2 (2004): 184-98. https://doi.org/10.1080/1470243042000325896.

Tougas, Marie-Louise. "Some Comments and Observations on the Montreux Document." *Yearbook of International Humanitarian Law* 12 (December 2009): 321-45. https://doi.org/10.1017/s1389135909000129.

UN General Assembly. *Universal Declaration of Human Rights*. Report no. UNGAR 217 A(III). 1948.

UN Human Rights Council. *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-*

Determination. Report no. A/HRC/15/25. July 5, 2010. https://digitallibrary.un.org/record/688383?ln=en.

United Nations General Assembly. *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*. Report no. A/HRC/15/25/Add.3. June 15, 2010. https://documents.un.org/doc/undoc/gen/g10/143/85/pdf/g1014385.pdf?token=ZcthrtcwHisjOga0eq&fe=true.

UN Working Group on the Use of Mercenaries. *Draft Convention on Private Military and Security Companies (PMSCs)*. Report no. A/HRC/WG.10/1/2. May 13, 2011. https://digitallibrary.un.org/record/707162?ln=en&v=pdf#files.

van den Berg, Bibi, and Dennis Broeders, eds. *Governing Cyberspace: Behavior, Power, and Diplomacy*. 2020. https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf.

van Meegdenburg, Hilde. "What the Research on PMSCs Discovered and Neglected: An Appraisal of the Literature." *Contemporary Security Policy* 36, no. 2 (2015): 321-45. https://doi.org/10.1080/13523260.2015.1061755.

Wassenaar Arrangement Secretariat, comp. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. Report no. WA-DOC (19) PUB 007. December 2019. https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.

Weber, Max, Hans Gerth, and C. Wright Mills. *Politics as a Vocation*. Hassell Street Press, 2021.

Weiss, Moritz. "The Rise of Cybersecurity Warriors?" *Small Wars and Insurgencies* 33, nos. 1-2 (2021): 272-93. https://doi.org/10.1080/09592318.2021.1976574.

Weissmann, Mikael, Niklas Nilsson, Björn Palmertz, and Per Thunholm. *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London, United Kingdom: Bloomsbury, 2021.

Westerwinter, Oliver. "Bargaining in Networks." *The New Power Politics*, August 1, 2016, 196-223. https://doi.org/10.1093/acprof:oso/9780190604493.003.0008.

White, Nigel D. "Outsourcing Military and Security Functions." *AJIL Unbound* 115 (2021): 317-21. https://doi.org/10.1017/aju.2021.45.