

UC Irvine

Analog Game Studies

Title

Serious Analog Game Development Across Disciplines

Permalink

<https://escholarship.org/uc/item/8298j9jv>

Journal

Analog Game Studies, 9(2)

Authors

Etheridge, Brian C.

Duncan, Christian

Mhire, Jeremy J.

et al.

Publication Date

2022-05-23

DOI

10.5070/V7.24IX89

Copyright Information

This work is made available under the terms of a Creative Commons Attribution License, available at <https://creativecommons.org/licenses/by/4.0/>



SERIOUS ANALOG GAME DEVELOPMENT ACROSS DISCIPLINES

Brian C. Etheridge, Christian Duncan, Jeremy J. Mhire, Jean Gourd, John Worsencroft, and Heath Tims

Abstract

In this essay, we share our effort to use serious analog game design as a means for breaking down academic silos, as a window through which these questions, and others like them, might be best approached. Much of the discussion and research in serious games and game-based learning have focused on proliferation and effectiveness of the format. This article focuses more on how serious analog game design promotes integrative learning through intentional faculty collaboration with one another. The initiative—the AICS project (Analysis and Investigations through Cyber-Scenarios)—was first developed and piloted at a regional university in 2012, building upon previous collaborative efforts between faculty of several colleges, and taking as its focus the development of real-time, immersive cyber-based or cyber-oriented simulations. AICS remains a genuinely rich case-study from which to draw best-practices not only for unique and timely content and curriculum design but also under what conditions (theoretically and practically) collaborative academic professional development can be encouraged and sustained.

Keywords

serious games, alternate reality games, ARG, higher education, cyberspace, AICS project, game design, government, security

Critics of higher education charge that the academy is too rigid and inflexible to meet the needs of a rapidly changing society. They claim that challenges facing social and environmental health and the needs of a rapidly evolving workforce require greater multi-disciplinary collaboration through innovative curriculum design and joint research projects.¹ In particular, government and industry experts highlight the need for greater multidisciplinary collaboration to recruit and train students in fields specific to cyberspace (e.g. computer science, electrical engineering, and cyber-security). This

¹ Ashley Bear and David Skorton, "The World Needs Students with Interdisciplinary Education," *Issues in Science and Technology* 35, no. 2 (Winter 2019): 60-62.

need arises because of the fields' core competencies and because the subject matter itself transcends a single disciplinary approach. Though perhaps not unique to cyberspace in principle, this need to encourage academic ecumenism has nonetheless created an unprecedented practical avenue for collaboration, as the domain itself crosscuts not only scientific and technical disciplines, but also disciplines in the traditional humanities, social sciences, and fine arts, among others. In other words, as the need for interdisciplinarity intersects with the digital domain, transcending disciplinary boundaries, whatever they may be, and promoting integrative learning becomes an operational necessity.²

While the need for multi-disciplinary collaboration is clear to many, the silo culture of higher education has remained stubbornly resilient.³ In what follows, we share our effort to use serious analog game design as a means for breaking down academic silos, as a window through which these questions, and others like them, might be best approached.⁴ Much of the discussion and research in serious games and game-based learning have focused on proliferation and effectiveness of the format.⁵ This article focuses more on how serious analog game design promotes integrative learning through intentional faculty collaboration with one another. The initiative—the AICS project (Analysis and Investigations through Cyber-Scenarios)—was first developed and piloted at a regional university in 2012, building upon previous collaborative efforts between faculty of several colleges, and taking as its focus the development of real-time, immersive cyber-based or cyber-oriented simulations. AICS remains a genuinely rich case-study from which to draw best-practices not only for unique and timely content and curriculum design but also under what conditions (theoretically and practically) collaborative academic professional development can be encouraged and sustained. To that end, Section II details the context and genesis of the AICS project, from its beginnings as a regional endeavor with the United States Air Force, through its conceptual phase as a Department of Homeland Security proof-of-concept initiative. Section III then elaborates the AICS model, drawing specific attention to the analytical dimensions of analog simulations that we designed for a cyber-context. Section IV offers lessons learned through the AICS project, including those incentives and opportunities integral to collaborative best practices. We conclude with a series of observations likely relevant to those seeking to encourage future collaborative efforts between faculty otherwise tethered to their disciplinary identity.

From the Beginning: The Context of AICS

It bears mentioning that the problem of academic “silos” is nothing new; organizing social interaction among faculty according to their research and teaching responsibilities is an outgrowth of

² On so-called “wicked problems,” see Brian W. Head, “Wicked Problems in Public Policy,” *Public Policy* 3, no. 2 (2008): 101–18; on the efforts by AAC&U around integrative learning see Ben Dedman, “From Learning Communities to Capstones: Faculty Leadership for Integrative Liberal Learning,” *Association of American Colleges & Universities*, March 1, 2019, <https://www.aacu.org/aacu-news/newsletter/2019/march/campus-model>; and on the formulation of Grand Challenges of the 21st Century see the National Academy of Engineering <https://www.popsi.com/scitech/article/2008-02/grand-engineering-challenges-21st-century>.

³ For a discussion of some possible approaches to breaking down silos around research, please see Elena Novak, Weinan Zhao, and Robert A. Reiser, “Promoting Interdisciplinary Research among Faculty,” *The Journal of Faculty Development* 28, no. 1 (January 2014): 19–24.

⁴ “Serious games” are often talked about in a digital game context, and so we use “serious analog games” here to highlight the distinct nature of our games.

⁵ Rosa Mikeal Martey et al., “Testing the Power of Game Lessons: The Effects of Art Style and Narrative Complexity on Reducing Cognitive Bias,” *International Journal of Communication* 11 (January 2017): 1635–60; Bradley E. Wiggins, “An Overview and Study on the Use of Games, Simulations, and Gamification in Higher Education,” *International Journal of Game-Based Learning* 6, no. 1 (January 2016): 18–29, <https://doi.org/10.4018/IJGBL.2016010102>; Riccardo Berta and Pablo Moreno-Ger, “Introduction: Intelligent Learning Assessment in Serious Games,” *International Journal of Serious Games* 5, no. 1 (March 26, 2018), 3–4, <https://doi.org/10.17083/ijsg.v5i1.237>.

the professionalization of the professoriate dating back to the late 19th century. In other words, as long as the academy has been divided into disciplines, faculty have tended to work together most closely with members of their own disciplines.⁶ When it occurred, collaboration was most often a disciplinary function driven by overlapping interests or research capacities. Still to this day, use of the word “multi-disciplinary” most often connotes work done between individuals within cognate fields (e.g. mathematics and computer science; biology and chemistry; philosophy and history). The successful fruit of multi-disciplinary collaboration in certain instances itself led to what was later called “inter-disciplinarity,” which suggested even greater coordination between conceptually clustered units, and which “generates an understanding of themes and ideas that cut across disciplines.”⁷ Given the continued articulated need for greater understanding around “wicked problems,”⁸ it seemed almost inevitable that the digital domain would give rise to what is now called “trans-disciplinarity,” suggesting a meeting-of-the-minds that crossed many if not all traditional disciplinary boundaries, and aimed at an understanding or meaning more comprehensive or synoptic in character. Indeed, a defining part of the AICS project has been its trans-disciplinary nature; trans-disciplinary work represents, according to the International Bureau of Education, an even higher level of integration that “dissolves the boundaries between the conventional disciplines and organizes teaching and learning around the construction of meaning in the context of real-world problems or themes.”⁹

Yet given the composition of and often rigid incentive structures associated with the modern university, it thus comes as no surprise that collaborative or “trans-disciplinary” efforts, though seemingly replete with potential, are nevertheless more often discussed than practiced. That these discussions have increased in frequency and duration, however, indicates a crucial insight—many of the social, technological, economic, and moral issues that beg today of scholarly insight and application are too large, too complex, and too diverse for a cluster of cognate disciplines, let alone for the faculty of a single discipline, no matter how large or well-funded. Nowhere is this seemingly more true than in cyberspace, whose issues range from national security and international competitive advantage, to commerce, communication, and digital currency, and even to privacy, property rights, stalking, bullying, and alienation. If there is one subject or phenomena that so easily exemplifies an emergent field that simultaneously cuts across and draws together many if not most academic disciplines, then surely it would be cyber.

But what exactly does the term cyber mean? Though no consensus definition has been reached on this question, it may help to outline several observations particularly relevant to the unique nature of the AICS project. Obviously, the word cyberspace conjoins the words cyber and space. Technically,

⁶ For a brief practical discussion of this challenge see Jeffrey H. Toney, “Break Down Academic Silos by Appealing to the Human Spirit,” *Dean & Provost* 11, no. 10 (June 2010): 4–5; for a deep discussion of disciplinarity and interdisciplinarity see Harvey J. Graff, *Undisciplining Knowledge: Interdisciplinarity in the Twentieth Century* (Johns Hopkins University Press, 2015).

⁷ Also, much of the interdisciplinary work in curriculum has been pursued through the promotion of learning communities, a high-impact practice. See for example, Emily Lardner and Gillies Malnarich, “A New Era in Learning-Community Work: Why the Pedagogy of Intentional Integration Matters,” *Change: The Magazine of Higher Learning* 40, no. 4 (2008): 30–37; “The Scholarship of Integration,” *ASHE-ERIC Higher Education Report* 29, no. 2 (April 2002): 45; Richard A. Gale, “Fostering Integrative Learning through Pedagogy,” *The Carnegie Foundation for the Advancement of Teaching* (2006): 1–13; Erinn Bentley and Jennifer Brown, “Transcending Disciplinary Lines to Promote Student Achievement at the Post-Secondary Level,” *International Journal of Teaching and Learning in Higher Education* 26, no. 2 (2014): 205–216.

⁸ See Head, “Wicked Problems in Public Policy.”

⁹ “Multidisciplinary Approach,” *International Bureau of Education*, accessed October 2, 2018, <http://www.ibe.unesco.org/en/glossary-curriculum-terminology/m/multidisciplinary-approach>; “Interdisciplinary Approach,” *International Bureau of Education*, accessed October 2, 2018, <http://www.ibe.unesco.org/en/glossary-curriculum-terminology/i/i/interdisciplinary-approach>; “Transdisciplinary Approach,” *International Bureau of Education*, accessed October 2, 2018, <http://www.ibe.unesco.org/en/glossary-curriculum-terminology/t/transdisciplinary-approach>; Jacqueline Y. Russell, John A. Harris, and Valerie A. Brown, *Tackling Wicked Problems Through the Transdisciplinary Imagination* (Earthscan, 2010).

the word cyber is not a word; “cyber” is a shortened form of cybernetics, which is the English equivalent of the Greek word *kybernetes*, which means to steer or navigate (it is also the root of the English word “governor”). Likewise, the word “space” comes from the Latin word *spatium*, which means room or place. Conjoining the words essentially creates a verbal noun out of a non-finite verb; rather than to steer or navigate to or in a place, cyberspace is a place in which one can steer or navigate.

To steer or navigate presupposes, however, the constraints of physical space; navigation is an activity that overcomes physical obstacles and hence moves from here to there. By making this verb into a noun, the word cyberspace creates a new concept: cyberspace is a domain of human operations that is theoretically unlimited by the physical environment, i.e. it removes the physical limitations on human actions, especially human communications. And it is for this reason that the domain of cyberspace so effectively cuts across disciplines; the very domain itself requires that we consider how our limitlessness in cyberspace relates to limits in physical space, overcoming limitations in certain circumstances while simultaneously introducing them into others.

Less theoretical, though more practically relevant, is the advent of the global network of computers and devices that comprise the internet, which represents a major leap forward in the ability of human beings to communicate. Often thought of as the second information revolution, on par with or maybe even greater than the impact of the Gutenberg press, the digital media of the internet offers such real-time interactivity among its users that the American military classified cyberspace as a fifth domain for engagement, elevating an immersive communication technology to the existing natural domains of land, sea, air, and space. In successive commentaries, the US Joint Chiefs of Staff talk about the cyber-domain as consisting of three interrelated levels: the physical layer, which constitutes the devices and infrastructure that comprise the network; the logical layer, which constitutes the data and information that make the network operational; and finally the cyber-persona layer, which represents the users, biological or automated, engaged in the domain.¹⁰

Given the nature of this new domain, and how it touches on and encompasses so much of our modern life, it is critical that we take innovative and multifaceted approaches to understanding and safeguarding it. In particular, in thinking about the user or human element, as many have pointed out, it is essential that we think about training and education at all levels, from ensuring cyber-hygiene, where users are trained to avoid the basic pitfalls of networked technology, to promoting issues regarding citizenship in the digital age, and finally to growing a cybersecurity pipeline to protect the infrastructure itself. To that end, the AICS project emerged from a long-standing initiative that seeks both to raise awareness about these issues and begin taking the first steps toward training a cyber-literate workforce. And as it stands, AICS is now one of the principle means of advancing teacher professional development and educational resources through the National Integrated Cyber Education Research Center (NICERC), which has been designated and funded by the Department of Homeland Security as its lead technical institution for Cybersecurity Educational efforts. Over the last several years NICERC has employed AICS and other intervention strategies to raise awareness and grow competence around key cyber-oriented areas, reaching 12,850 teachers across all fifty states by 2018.¹¹

¹⁰ Joint Publications 3-12: Cyberspace Operations, June 8, 2018, https://fas.org/irp/doddir/dod/jp3_12.pdf.

¹¹ Sean Green, “CIC, NICERC Get Grant Worth Millions to Expand Efforts across the US,” *Bossier Press-Tribune*, accessed October 3, 2018, <http://bossierpress.com/cic-nicerc-get-grant-worth-millions-to-expand-efforts-across-the-us/>; Tim Hwang, *Digital Disinformation: A Primer* (Atlantic Council, 2017), http://www.atlanticcouncil.org/images/Digital_Disinformation_Primer_web_0925.pdf; “What Can Citizens Do To Fight Foreign

Before moving to the specifics of the AICS model, a few words are in order regarding its history, especially given its rather unique design. AICS is the culmination of a series of initiatives oriented toward developing a common framework for teaching and learning about the nature and challenges associated with cyberspace as a discrete environment. The predecessor to AICS—Cyber Discovery—launched in 2008 as a collaboration between faculty from mathematics, engineering, computer science, history, political science, literary studies, sociology, and architecture. Using a game-based learning format adapted to cyberspace, Cyber Discovery created a week-long immersive, residential experience for small teams of high school teachers and students. The educational content was structured around week-long challenges involving cryptography, robotics, and social and ethical issues connected to networked technologies. The curriculum was also supplemented through the production of integrated cultural products that depict the nature of cyberspace (e.g. performance skits, 3D modeling, robotic augmentation). Taken together, Cyber Discovery's activities were designed to create a seamless experience in which teachers understand and explore the relationship between the virtual and the kinetic worlds, wrestle with the ways in which cyber activity is redefining relationships, identities, and institutions, and experiment with various strategies for encrypting and decrypting information.¹²

Cyber Discovery's dynamic structure—its game-based format adopted and adapted through diverse faculty participation—led to a desire for further integration built more intentionally around a cyberspace threat. Out of this desire came AICS (Analysis and Investigation through Cyber-based Scenarios), which is also based on gamified learning. But this time, the experience is much more structured as a serious game, in which participants are thrust into immersive, real-time simulations that occur in functionally equivalent, parallel worlds.¹³ In these simulations, student-teacher teams are cast as government officials confronted with a possible cyber attack; the “smart” controls of a hydroelectric dam suddenly opens the floodgates, threatening lives and infrastructure; disaffected State Department employees leak sensitive material to a major news outlet, potentially damaging US-Mexico relations; or the system that controls a drawbridge in Chicago malfunctions in the middle of a peaceful protest march, injuring dozens. Over the course of three to four hours, the teams receive successive rounds of evidence (briefings) regarding the incident and are then asked to prepare a briefing that articulates and justifies their interpretation of the event. Working together both to create the immersive game and to deploy the simulation in “real time,” participating faculty co-construct trans-disciplinary challenges and support structures to engage students in grappling with the issues associated with participating in and securing the cyber realm.

In some ways, AICS can be thought of as one form of an Alternate Reality Game (ARG). In an ARG, game players collaboratively work through prefabricated parts of the game (known as artifacts), solving plot-based challenges and puzzles and advancing the storyline (often determining its ending). Although the players are external to the game, they have an internal contribution in that they help to shape it during gameplay. ARGs take place in real time and make use of transmedia when representing artifacts, allowing players to consume various types of resources and coordinate real world and online components. They are inherently complex, not easily solvable by a single

Disinformation Campaigns?,” NPR.org, accessed October 2, 2018, <https://www.npr.org/2018/10/01/653264175/what-can-citizens-do-to-fight-foreign-disinformation-campaigns>.

¹² Brian C. Etheridge et al., “Studies in Cyberspace: Honors, Professional Teacher Development, Curricular Development, and Systemic Change in Louisiana,” *Honors in Practice* 6 (2010): 189-201.

¹³ Perhaps contrary to first appearances, the usage of parallel worlds in the simulations is both highly effective and logistically necessary. Regarding the latter, creating fictitious events with a high degree of believability requires adapting as much of our world into a simulated environment. The fictitious events thus gain their plausibility precisely because of how probable they are in a cyber-based world.

participant, and are effective at engaging groups of people in a collaborative way, enabling experiential learning along the way.¹⁴

ARGs typically feature decentralized authorship, allowing a game to be dynamically shaped by many collaborating players during gameplay. Usually, a “puppet-master” designs the game, providing resources and obstacles for the game players. A “curtain” serves as a “fourth wall” metaphor to separate the puppet-masters from the game players – although it can be pulled back when necessary so that designers can interact with players to disambiguate gameplay, for example.¹⁵ Although ARGs are inherently games, the view by designers and players of ARGs is that they are not really games at all – or more specifically, that they should not *feel* like games at all. This is especially true of *serious* ARGs,¹⁶ whose storyline is plausible (which is what makes them *serious* ARGs).



Figure 1: Photo taken during the creation of the 2022 AICS. Image used with permission by the author.

In AICS, participants collectively solve a scenario whose storyline is plausible, akin to a serious ARG. Creators (as trans-disciplinary as they may be) craft scenarios whose artifacts serve to both support and challenge the participants. The diverse artifacts take many different forms that require participants to bring their collective expertise to the table, sharing their interpretation of artifacts and solutions in real time. The process is very organic and dynamic, often leading the players to either include or exclude artifacts very quickly. A “curtain” exists by way of the role-playing process during dramatic time. Participants and facilitators transition from real time to dramatic time during

¹⁴ Nicole Whitlock, “Alternate Reality Games for Developing Student Autonomy and Peer Learning,” Paper presented to Learners in the Co-creation of Knowledge (LICK), 2008, http://www2.napier.ac.uk/transform/LICK_proceedings/Nicola_Whitton.pdf.

¹⁵ S. Conway and T. Innocent, “Urban Codemakers: Decompiling the Player,” *Analog Game Studies* 3, no. 2 (2016), <https://analoggamestudies.org/tag/alternate-reality-game/>.

¹⁶ See <http://pitchfork.com/features/get-that-out-of-your-mouth/6586-get-that-out-of-your-mouth-34/> and <https://www.mercurynews.com/2007/04/30/takahashi-slick-way-to-address-oil-thirst/> for examples of serious ARGs.

scenario deployment and take on the persona of various government agents. Inevitably, participants sometimes ask questions related to gameplay. This presents an opportunity for facilitators to essentially pull the curtain back, briefly pausing their role as agents, to provide participants with meta-information to disambiguate gameplay. These discussions sometimes result in real time tweaks to a scenario with the potential to alter subsequent briefings (i.e. change the storyline). Moreover, as a scenario plays out, facilitators may dynamically react to the actions and decisions of participants, enabling a scenario to evolve as it is being played. To some extent, as the participants organically “play” through a scenario, they may influence its storyline.

This is reinforced in the final participant briefings (which could be considered potential endings of a scenario). Teams of participants must answer three main questions (who did it?, why did they do it?, and what should the U.S. response be?), which connects a scenario with its plausible potential to have real impact on our nation-state. Participants must carefully answer these questions in the context of the real world. In essence, what would a realistic U.S. response be if this scenario had actually played out? The creators take great care to design scenarios that are plausible, even if some of the artifacts provided in briefings are fictitious.

Similar to ARGs, AICS scenarios are intentionally constructed such that artifacts are not delivered in any particularly meaningful order. That is, a scenario does not necessarily play out coherently. Briefings include evidence and artifacts that are delivered as they would likely be by analysts in the real world (i.e. information is disseminated to participant investigators once it is found, collected, analyzed, and organized by analysts). Participants assemble these artifacts, trying to impose some sort of meaningful order to try to determine the details of a scenario. Creators design the briefings to reveal a scenario in stages. Although this is designed to mimic a real-world event (i.e. information is not all available at once), it also brings in a level of realism (e.g. resources are not limitless).

The creators of a scenario are on-hand throughout its deployment. This allows a scenario to evolve somewhat based upon the actions of the participants. In other words, there is opportunity for participants to control how the plot unfolds. At certain times during gameplay, participants have the opportunity to ask carefully crafted questions. In some scenarios, briefings are dynamically ordered based on how participants ask questions (i.e. ask the right question, and the most helpful briefing is delivered first; ask a wrong question, and it is delivered last). This gives some participants a slight advantage in that they receive more relevant information before others, allowing them to exclude irrelevant actors and narrow things down earlier. Responses to questions, provided in real time by creators and facilitators, are often used to steer teams in interesting directions and often require creating new scenario artifacts on the fly, potentially altering the scenario’s storyline. Often, discussions overheard among the participants by facilitators may lead to organic actions in dramatic time during a scenario’s deployment. During one scenario, for example, a facilitator playing the part of a DHS agent was determined by a team of participants to be a bad actor in that scenario. Although the creators of the scenario never predicted this to happen, it afforded an opportunity for the facilitators to “go along with it,” affecting the scenario’s storyline and ending. Ultimately, the DHS agent was “arrested” during the team’s final briefing (which led to an interesting dynamic, obviously replete with overacting), even though that was not an intended goal of the scenario. In effect, a final team’s briefing may be considered one possible “ending” of a scenario (it may be interpreted in

various ways, with one obvious “correct” way as intended by the creators). This is similar to many past ARGs such as *ilovebees*¹⁷ and several that were based on the TV series *Alias*.¹⁸

Admittedly, there is much less room in AICS for participants to significantly influence a scenario than there is in an ARG. Although it is true that the actions of participants may influence the direction of a scenario as it is deployed, the very nature of a scenario’s design limits the degree to which it can change during deployment. Instead, lessons learned at the conclusion of a scenario are fed back through the creative process, allowing the creators to improve the scenario for future deployments.

The Framework of an AICS Scenario

In an important sense, the entire AICS project revolves around the scenario. We work in diverse teams to design and create internally consistent cyber-based simulations for use in residential camps, and increasingly in classroom-based applications.¹⁹ The efficacy of that collective effort is made possible through an organizational scaffolding that clearly differentiates phases within an iterative creative process. In general, the development of these serious analog games follows the general framework of backwards design popular in course and curriculum construction. For the purposes of illustration, we will first describe the gameplay associated with a scenario from 2014 and then shift to how the scenario was developed.

Each scenario centers around an *event* that has occurred somewhere in the world. Faculty teams are involved in both the generation of scenarios but also play roles in gameplay. *Creators* are responsible for the creation of the scenario, *facilitators* execute the scenario by handing out information and judging the final analysis, and student *participants*, who work in teams to solve the case. In our example (hereafter highlighted in italics), the various players interact in a dramatic turn-of-events: *the example scenario begins with the participants learning the Turkish president has been attacked by a NATO drone.*

The goal of every scenario is to answer three overarching questions: Who committed the act? Why did they do it? And, what should the (governmental) response be? In general, the “who” and “why” are known by the creators but the “response” is necessarily open-ended. *In our example scenario, it is quickly determined that the drone was compromised, leading to the three big overarching questions. If it wasn’t NATO, who was it, why did they do it, and what should we (the federal government) do about it?* Each scenario has multiple potential suspects responsible for the event. We refer to these suspects as *actors* and broadly categorize them as an individual, a state, a non-state, and chance (referred to as a non-starter). When the scenario is created, the development team chooses one particular actor, which sets the theme for that scenario. Except for the non-starter, the actors are fairly self-explanatory. In the non-starter, an event occurs which has no actual actor; it happens by chance. For example, either an accident or act of nature initiated the event. *It is possible (though soon ruled out) that the drone simply malfunctioned. But it is more likely that someone or some group is behind the attack.*

¹⁷ J. Kim, J. Allen, and E. Lee, “Alternate Reality Gaming,” *Communications of the ACM* 51, no. 2 (2008): 36-42, <https://doi.org/10.1145/1314215.1314222>. See https://en.wikipedia.org/wiki/I_Love_Bees and https://halo.fandom.com/wiki/I_love_bees for more details.

¹⁸ H. Örnebring, “Alternate Reality Gaming and Convergence Culture: The Case of *Alias*,” *International Journal of Cultural Studies* 10, no. 4 (2007): 445-462, <https://doi.org/10.1177/1367877907083079>.

¹⁹ Beginning in 2016, NICERC began the process of repurposing the existing scenarios as modules that could be more easily employed by teachers in their classrooms.

After the initial event has been presented, the participants are provided materials related, possibly tangentially, to the event. Every round of new materials is referred to as a *briefing*. The first briefing provides the basic event known to the general public as well as a few inside pieces of information. *The participants are presented with an internal memo from the US general heading NATO's Air Force command to the Secretary of the Air Force detailing that they had lost control of the advanced drones, which had gone stealth and attacked a building in Istanbul.* After this initial briefing, details arrive in a seemingly chaotic order as if they are given as soon as the information becomes available. The information can range greatly including internal memorandum, government and industrial press releases, (possibly intercepted) private communication, social media posts, and international communications, and can contain valid, invalid, conflicting, and potentially misleading information.

Central Intelligence Agency

Internal Memorandum

To: Undersecretaries; Agency Liaisons

From: John Brennan

Subject: Memo of Cooperation

Date: 07/25/14 3:52 p.m. (CDT)



All,

A drone has attacked two sites in Turkey – the first is a major Turkish natural gas facility and the second is the adjacent Turkish military base which houses medical, security and transportation facilities. The gas facility is a nexus point where supplies from Iran and Iraq come in to be processed and dispersed.

JB

Figure 2: Example of a sample AICS document. Image used with permission by the author.

The information the participants receive is designed to have a *needle-and-haystack* relationship. The overwhelming majority of the information is intentionally irrelevant, leaving the participants to discover the true needle within this informational haystack. Further extending the needle metaphor, multiple threads weave through the story. Each thread ties one particular actor to the event, but only one thread actually connects with the needle. The others are frayed and broken, some in more

obvious manners than others. *One dead-end thread involves the connection of potentially leaked government information to a fictitious blog-writer named Ethan McMahan, writing for the blog Real American Patriots. Only later do the participants learn that the information was based solely on the blogger's conjecture, and not on factual evidence or testimony.* However, the creators purposefully withhold some key information that may not be necessary to complete the thread but strengthens the thread's connection to the needle.

To capture the notion of limited resources, the facilitators give the participants the opportunity to pose a small set of fact-finding questions before the final briefing. *One team having focused their investigation on a set of companies responsible for the development of the drones posed the following question: "Can we have email records including metadata from Ocsic and Drone, Inc?"* After a period of time, the facilitators provide responses to the participants. Internal to the development process, the creators try to anticipate certain questions, typically the ones most likely to be useful or known dead-ends, and write valid responses, leaving unanticipated questions for the facilitators to answer in real time. These question sets provide the teams on the right track an opportunity to acquire the missing key information, strengthening their case. But it is also a chance for the facilitators to help steer other teams onto the correct thread, or at least off a wrong thread.

After receiving and assessing the last briefing, the participating teams must debrief a (hypothetical) panel of officials, for example, representatives of Homeland Security. Comprised of facilitators, the panel might also include guest representatives with limited knowledge of the scenario. Each team must present to the panel the facts as they understand them and their answers to the three overarching questions as well as providing evidence supporting their assertions. In a typical format, this is a back-and-forth process, where the panelists question the teams on their findings in an attempt to deliberate the veracity of their assessment and determine what exactly needs to be done in this situation. *One team might (wrongly) believe that Ethan McMahan was involved in providing material evidence about drone encryption keys to an Iranian government official but acknowledge their lack of evidence connecting the two and suggest that Mr. McMahan be apprehended and questioned for security reasons. And another team might (correctly) point out that a Turkish academic researcher named Khalid Mehmet, working in Turkey but having previously worked at various US research labs connected to the development of the drone technology, had essentially compromised the drone's underlying security system and sold that information and access to a group of Turkish military generals attempting to initiate a military coup. They might then determine the best course of action is to ground and patch all related drones, work with the Turkish government to prevent the coup, and urge the government to detain Mehmet and the generals directly involved in the coup.*

After hearing the presentations, the panelists judge the teams based on the strength of their arguments, the confidence and understanding of the material (particularly in how they respond to the panelists' questions), and how well they addressed the three overarching questions. Often a team might identify the correct thread but lay out their case poorly, missing vital supporting documents or providing extremely unrealistic suggestions for a response to the incident. But, other times, a team might not identify the correct thread, but lay out clearly their evidence, and state plainly where their assertions are lacking evidence, where the evidence is circumstantial, and how their response is mitigated by the information gap. In an earlier scenario, one team believed, without evidence, that a particularly unpleasant individual was behind a cyber attack and strongly suggested that the individual be apprehended and tortured until a confession was obtained. After hearing other teams' cases and learning the true actor involved, that team quickly learned to base their response on the strength of the evidence they had.

DCN: 3751

THE SECRETARY OF DEFENSE

**1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000**

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ADMIRALS OF THE NAVAL COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
DIRECTOR OF THE DEPARTMENT OF HOMELAND SECURITY

SUBJECT: unmanned aircraft strikes in Turkey

BEGINNING AT 0840 CDT NATO ALLY TURKEY EXPERIENCED AN UNMANNED AIRSTRIKES ON A CIVILIAN TARGET. THE STRIKE APPEARED TO BE DIRECTED AT A DIPLOMATIC TARGET. THE STRIKE APPEARS TO HAVE BEEN CARRIED OUT BY AIRCRAFT SIMILAR TO THOSE DRONES PROVIDED TO NATO BY THE UNITED STATES.

SECRETARY OF DEFENSE ORDERS ALL USAF BASES TO INVENTORY AND ACCOUNT FOR ALL DOMESTIC AND FOREIGN STANDING DRONES. COMBAT READY ASSETS SHOULD PREPARE FOR POSSIBLE DEPLOYMENT.

AGENCY HEADS ARE HEREBY NOTIFIED THAT THE THREAT LEVEL HAS INCREASED FROM MODERATE TO SIGNIFICANT.

Figure 3: Example of a sample AICS document. Image used with permission by the author.

The development of a scenario is a complex task requiring expertise across diverse disciplines. Consequently, scenario creation is a trans-disciplinary process by necessity, and a team's composition becomes theoretically unlimited. For example, a typical creation team might consist of faculty members from English, engineering, computer science, political science, and history. In backwards design fashion, the process begins by identifying the intended learning outcomes and then developing an overarching scenario that provides the students with the opportunity to learn and practice the skills identified with the outcomes. Often, the stories are ripped-from-the-headlines—one scenario begins with the question of how to incorporate recent friction between online shopping behemoth Amazon and workers' rights advocates; another is set at the Trump International Hotel in Washington, DC, a magnet for criticism and negative press. These real-life touches give participants a sense of plausibility—they've heard this story before—and in developing the overall story, potential instigators are enmeshed in these true-to-life worlds, forming the primary threads. For each thread, the creative team determines the motivation, the access, and the ability to carry out the event. Since only one thread represents the true instigator, the credibility of each need not be realistic. The threads encompass a wide range of actors, from the individual to the non-state to the state and could leave open the possibility that it is simply a chance accident. To make the investigative task challenging but not impossible, some threads must go deeper than others, which can be accomplished by creating more evidence for some rather than others.

Early in the process, the true actor must be identified, helping focus the creation. For this particular thread, credible evidence must be identified—a series of documents, communications, reports—clearly laying out the answer to the first two overarching questions and guiding the formation of the needle. All other threads need not be sound as they all by necessity have holes or lacuna in them. Here we occasionally use foils that traffic in stereotypes or tropes—jihadist terror groups of Middle Eastern origin, or crunchy granola-types who lead shadowy eco-terrorism organizations—that might trick participants into wasting time on these too-easy leads. Following the establishment of the main threads, the creators then outline a basic timeline of key events, both for the primary and secondary threads. The creators have to break the timeline down into three distinct periods, the period before the event, during the (initial) event, which triggers the investigation, and during the unfolding investigation, with the latter adding a sense of urgency to the scenario. *In our scenario, several drones were still missing and continued to make periodic attacks with the potential for further damage.*

A master document is created that frames the timeline, allowing the creators to see the narrative of the scenario, though obviously not available to the participants. Several documents must be written to reveal the story. Modeling reality, these documents come from various sources, in many different formats, and arrive in non-sequential order. Some of the most commonly used sources in the scenarios include news articles, news broadcasts, press releases, dossiers, bios, technical documents, opinion pieces, social media blogs and commentaries, email exchanges, and transcripts of in-person interviews. The first step in the process is creating a list of documents that have to be created. This requires establishing the needle, the documents that will identify the actual actor and which reveal what really happened, though some aspects can be left for speculation.

The Daily Telegraph

Istanbul hotel explosion: President Erdoğan feared dead!

July 25th, 2014 9:01 a.m. (CDT)



Workers inspect the inside of the shattered hotel.

Rush hour in Istanbul was shattered this afternoon by an explosion at the Marmara Hotel. While it's unclear as of yet what happened, one thing is clear. Nothing here will ever be the same again. This hotel was the home of President Tayyip Erdoğan, whose presence was confirmed by hotel staff willing to speak with our sources following the blast. Recep Tayyip Erdoğan could not be reached for comment, nor could the Telegraph confirm his well-being. We will stay on the scene and report what we find throughout the day.

Figure 4: Example of a sample AICS document. Image used with permission by the author.

The next step is creating the haystack, the documents that complicate the investigation. Depending upon the scenario, the complexity of the haystack may require the generation of over one hundred documents. Varying in credibility, these documents strengthen the case for other threads, but should all lead nowhere at some point, or at least never completely connect in any manner as strongly as the needle. The documents that form the haystack should include elements of surprise, with revelations and misunderstandings. But there should also be elements of pure speculation, e.g. online blogs posing conspiracy theories or claims of "facts" with no grounding in reality or evidence. The purpose, of course, is to get participants to question the credibility of their sources. To be sure, the speculation can sometimes be correct, though corroborated only with additional supporting evidence. In turn, additional evidence often shows the speculation as mere speculation, and hence

that the thread does not fully connect. But most importantly, these documents are meant to confound the participant.

Along with the timeline and main document list, the creators have to develop and document a list of primary characters—for example, individuals, organizations, corporations, and governments. These characters are essential for keeping the story internally consistent. As with documents retrieved in any real investigation, there can be errors (intentional or accidental) but these should be minimal. To keep the list of characters closely tied to the master document during development, a creator must be vigilant in documenting all newly introduced characters. The creation of a set of standard templates also provides a more uniform feel and consistency to the scenario.

Once the timeline, document list, and character list are created, the individual creators within a team can begin to divide up the large task of creating the documents based on their interests and individual specialties. For example, faculty from engineering might contribute technical documents, such as schematics, diagrams, or computer logs. When generating the documents, the creators must also determine a briefing timeline, outlining the particular time a document can be handed out. This order must be consistent with the scenario timeline and the investigative timeline. The former is most important for unfolding events—*A news article about a subsequent drone attack on a Turkish military hospital, housing the injured Turkish president, cannot appear in a briefing before the event actually happens.* The latter is important for making the investigation realistic—*A dossier on Khalid Mehmet cannot be provided until he has been identified as connected in some form to the drones that attacked.* Generally, once a document is established in a specific briefing, it can usually be pushed back to a later briefing but rarely to an earlier briefing. This movement allows for balancing the document load for the participants. In early incarnations, we often front-loaded the documents, drastically overwhelming the participants in the early briefings and providing little information of substance in the latter briefings. The balancing has allowed us to fine-tune that approach giving equal amount of material at each stage. It is also important that the documents comprising the needle be laid out gradually. The participants must be able to connect the primary thread fully by the final few briefings, but the needle cannot arrive all at the end either. In addition, there should also be a gradual elimination of other threads. Whereas in the early briefings the participants might have a dozen potential suspects, by the later briefings there ideally would be only two or three possible suspects remaining.

The delivery of the needle documents must also be coordinated with the fact-finding question period, to help model the limited resources of any investigation. Participants, of course, may ask any questions they wish, but the piece of connecting evidence and the possibility of its existence must be somewhat realizable (but not immediately obvious). The needle documents presented up until that point should guide the way to the missing piece without being too obvious. *In our example scenario, there existed an email communication from an employee at Drone, Inc. that implicated him in a potential cover-up of some security flaws. In the story, Drone, Inc. was cooperating and willing to provide batch email communications but the request was not made by DHS, unless a team specifically requested it as a fact-finding question.*

The creators must also take care to design the needle to be internally consistent and coherent to the scenario's narrative. Often an action taken by a character seems intuitive and rational initially, though once documented it becomes questionable, requiring a different tact or strategy. A character whose reputation seemed unimpeachable in earlier briefings can later be found to have a checkered past—a run-in with the law years ago involving an activity that is uncannily similar to activities documented in the briefings—which can have ripple effects throughout the scenario, altering other

characters and situations in various ways that are hard to predict. The needle documents must therefore be designed and created before most other documents to limit unnecessary changes, but changes can and will happen.

Although there are numerous ways one might approach developing scenarios, it is important to emphasize how crucial iteration is to any process. With AICS we have employed a three-stage process, where each stage takes place over a weekend during the academic year. In the first stage, teams meet as a collective group to create the basic framework of each scenario. Each team begins by brainstorming their event, and then fleshing out the details of a story that explains the who, how, and why. Each then presents their scenario narrative to other development teams, providing the opportunity to test nascent scenarios for internal consistency and plausibility, as well as preventing any two teams from creating similar scenarios. During the second phase, each team fleshes out the general details of the scenario and engages in the process of document generation outlined above. In the final phase, the teams again meet collectively and take turns play-testing each of the scenarios, looking for errors, inconsistencies, missing documents, etc. This third phase also allows the creators to gauge the efficacy of their scenario, evaluating the quality of the generated documents and identifying plot holes, points of confusion, the clarity of the “needle,” and complexity of the “haystack.”



Figure 5: Photo of playtesting, AICS 2022. Image used with permission by the author.

Conclusion

We originally developed the AICS model as a means to use serious games to educate and motivate students to think about the broader context of cyber-security, but it grew into something far greater. The process of creation itself quickly became an education for the creators, a means for people from vastly different disciplines to collaborate and learn about the strong connections each discipline had to cyberspace. What we have presented in this article is a guide, a means to help others recreate what we have done in the hopes that they can also benefit from the experience of the trans-disciplinary development of a serious game in their own domain.

Over the years we have learned many lessons. For example, originally the scenarios' core concepts were developed by two members only and others were brought in to help in the massive undertaking of document generation. But once all team members were involved in the initial creation process, there was considerably more buy-in and ownership of the time-consuming development process. The creation process itself was developed over time. Play-testing was another key addition to the process. Initially, all scenarios were first tested live. Without it, the creators had difficulty identifying every hole in the logic, gauging the difficulty or ease of a specific scenario, and adjusting the scenario to the proper complexity level.

The model is naturally still evolving. But in recent years, we looked to expand the process in various directions. In particular, we started the process of converting scenarios into a format suitable for a high school curriculum. Our scenarios have always focused on high-school age students and their teachers but the format is not directly suitable for a 50-minute classroom period. So, previous scenarios have been stripped down to essential documents while still maintaining the nature of the project. Certain scenarios have also been tested in college-level curricula. Spaced out over several weeks, these scenarios incorporated outside work with class-time deliberations. Although these scenarios have been designed for a week-long summer camp, there is also potential for a weekend single-day competition, where students first practice prior scenarios before attempting the one-day competition.

Perhaps our greatest lesson has been that game design and development is an ideal vehicle for interdisciplinary collaboration and integrative learning opportunities for students. Faculty teaching in learning communities could look to serious games as potential integrative assignments that tie the courses together.²⁰ Faculty committed to recovering the notion of a core might consider serious games as a complement to a great books curriculum. And faculty devoted to exploring wicked problems or grand challenges can use serious games as a simulation for preparing students to do transdisciplinary research. In these examples, as in others, serious games can provide enriching opportunities for faculty and students alike and go a long way toward breaking down academic silos that have historically and artificially fractured human curiosity and creativity.



Brian C. Etheridge is Professor of History and Director of Institutional Effectiveness and QEP at Kennesaw State University. He has been engaged in interdisciplinary initiatives through his work in honors, educational development, and academic innovation. He has written widely about American foreign relations history, teaching and learning, and cybersecurity education.

Christian Duncan is a Professor of Computer Science and the Director of the BS in Computer Science Program at Quinnipiac University where his instruction covers many aspects of computer science including introductory courses in programming, algorithms, graphics, and security. His primary research is in the areas of graph visualization and computational geometry.

Jeremy J. Mhire is the Joe D. Waggoner Professor of Political Science and the Director of the Waggoner Center for Civic Engagement and Public Policy at Louisiana Tech University. His teaching and research areas cover the history of political thought, political philosophy and theory, and democratic theory and engagement.

Jean Gourd is a Professor of Computer Science and the Chair of the Computer Science Department at The University of Tampa. His research interests are in the areas of computer science curriculum development (including pedagogy), project-based learning, cyber security, distributed computing, software engineering, and artificial intelligence. During his career, Dr. Gourd has received over \$6.5M in research funding for activities that involve foundational research in computing, applied projects in computing and cyber security, and educational activities. He has one patent under review and many publications in peer reviewed journals, published at conferences, and as chapters in books. He has also published a textbook that covers the Science of Computing and serves as the primary source for an innovative freshman curriculum in computing.

John Worsencroft is assistant professor of history at Louisiana Tech University. He holds a BA and MA in history from the University of Utah, and he received his PhD in history from Temple University.

Heath Tims is the Associate Dean for Undergraduate Studies in the College of Engineering and Science, and an Associate Professor of Mechanical Engineering at Louisiana Tech University. He also holds the endowed Cajun Contractors Professorship. He received his B.S degree from Louisiana Tech University and his M.S. and Ph.D. from the University of Texas at Austin. Dr. Tims' research focuses primarily on engineering education and multidisciplinary collaborative projects.