2022

An Analysis of Cyber Wargaming: Current Games, Limitations, and Recommendations

Sarah Chen

Claremont McKenna College

An Analysis of Cyber Wargaming: Current Games, Limitations, and Recommendations

Submitted to
Professor Jennifer Taw

By
Sarah Chen

For
Senior Thesis
Fall 2021-Spring 2022
April 25, 2022

Acknowledgments

Professor Taw, thank you for being my champion during these four years at Claremont McKenna College. Without your guidance and support, I would not be the person I am today. You took a shy, quiet bookworm with a love of science-fiction and videogames and helped her find her passion for wargaming, cyber conflict, and the intersection between the two.

I would also like to thank the wargaming community and all the experts that volunteered their time to speak with an aspiring wargamer. A particular shoutout to Sebastian Bae, for encouraging my interest in wargaming and inviting me to countless Georgetown Wargaming Society events, as well as Yuna Wong and the Women's Wargaming Network.

To Dharkann, may we always have the energy of Sheila, Kalani, and Machiavelli, and to my younger brother, Kevin, for when he has to write his own thesis and will finally understand why every time we called I was in the computer lab, had just left the computer lab, or was going to the computer lab.

Contents

Abstract

Cyberspace operations and conflict pose a unique challenge to decision-makers due to the uncertainty and unpredictability of cyber capabilities. Relying on wargaming literature, public cyber wargame reports, and expert interviews, this thesis analyzes the utility of cyber wargaming for education and analysis. Cyber wargames offer a method of testing, exploring, and understanding cyberspace through the abstraction and representation of cyber tools and attack cycles.

The thesis begins by examining cyber conflict and theorizes hypothetical wargame use cases. It then creates a framework for cyber wargaming elements and examines the design of eleven analytical wargames, eight educational wargames, and three commercial games according to this model. Lastly, the paper looks at the limitations and problems of cyber wargaming, relying on interviews with wargame designers, and suggests solutions going forward for future cyber wargame design and publication.

Chapter 1. Why build cyber wargames?

On July 27, 2021, President Joe Biden warned, in a speech at the Office of the Director of National Intelligence, that "I think it's more than likely we're going to end up, if we end up in a war - a real shooting war with a major power - it's going to be as a consequence of a cyber breach of great consequence and it's increasing exponentially, the capabilities."[1]

The United States has recognized cyberspace as an operational domain for over a decade, and the budget for cyberspace investment has consistently grown. The Pentagon asked for 11.2 billion dollars in the 2023 fiscal budget for cyberspace activities, in the wake of a discovery that Russian government-backed hackers had targeted American defense contractor systems over the last two years.[2]

Cyberspace operations threaten sensitive data and have started targeting the command and control or operation capabilities of critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) keeps a list of alerts on critical infrastructure threats. The BlackMatter ransomware has targeted critical infrastructure, including food supply chains, in the United States in 2021, there are ongoing threats to

[1] Nandita Bose, "Biden: If U.S. Has 'real Shooting War' It Could Be Result of Cyber Attacks," *Reuters*, July 28, 2021, sec. World, https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/.
[2] Jaspreet Gill, "Pentagon Wants $11.2B for Cyberspace Security, Training in FY23," *Breaking Defense* (blog), March 30, 2022, https://breakingdefense.sites.breakingmedia.com/2022/03/pentagon-wants-11-2b-for-cyberspace-security-training-in-fy23/; Lee Ferran, "Russian Hackers Raided Defense Contractors for Two Years, Stole Sensitive Info: US," *Breaking Defense* (blog), February 16, 2022, https://breakingdefense.sites.breakingmedia.com/2022/02/russian-hackers-raided-defense-contractors-for-two-years-stole-sensitive-info/.

U.S. water and water waste systems, SolarWinds resulted in Russia gaining access to U.S classified information, and DarkSide ransomware threatened pipeline infrastructure.[3]

Hacking has also become relatively resource cheap and 'easy.' In 2013, Thomas Rid, author of "Cyber War Will Not Happen," published a newspaper article detailing his five-day hacking crash course at Idaho National Labs: "Why hacking is way too easy."[4] On the fourth day, the workshop attendees, Industrial Control Systems operators, were split into the red and blue teams to defend a mock chemical company and by 5 PM, the red team had succeeded in infiltrating and releasing chemicals into the plant. Thomas Rid raises the concern that hacking is too easy, particularly given the connection of many critical industry control systems to the internet. Rid brings up Shodan, an open search engine, which has been "Google for Hackers" because it shows open ports and accessible IP addresses for devices connected to the internet. In the year of publication, Shodan listed control systems for nuclear power plants, a particle-accelerating cyclotron, a city's traffic system, and a hydroelectric plant.[5] A May 2015 visualization of industrial control systems on Shodan by John Matherly, the creator of Shodan, found over 20,445 ICS devices, lighting up the United States.[6]

---

[3] CISA, "Official Alerts & Statements - CISA | CISA," 2022, https://www.cisa.gov/stopransomware/official-alerts-statements-cisa.
[4] Thomas Rid, "Why Hacking Is Way Too Easy," The Sydney Morning Herald, July 31, 2013, https://www.smh.com.au/technology/why-hacking-is-way-too-easy-20130726-hv153.html.
[5] David Goldman, "Shodan: The Scariest Search Engine on the Internet," CNNMoney, April 8, 2013, https://money.cnn.com/2013/04/08/technology/security/shodan/index.html.
[6] John Matherly, "State of Control Systems in the USA," Shodan Blog, May 15, 2015, http://blog.shodan.io/state-of-control-systems-in-the-usa-2015-05/.

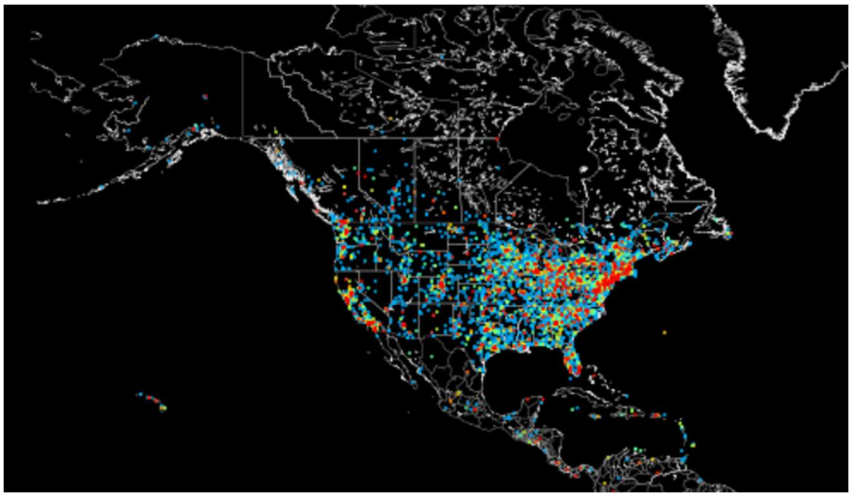

Figure 1. 2015 Visualization of Industrial Control Systems Connected to the Internet.[7] (John Matherly, "State of Control Systems in the USA," Shodan Blog, May 15, 2015, http://blog.shodan.io/state-of-control-systems-in-the-usa-2015-05/.)

While Shodan itself is less of a concern because the same penetration and surveillance could be conducted by bad actors via botnets, the concern is that critical infrastructure's command and control systems are too connected to the internet in the United States.[8] As cyber attacks become more severe, threatening, and relevant to conflict, decision-makers must be able to predict, prepare, and respond to cyberspace threats. The United States is vulnerable, and wargames offer a way to playtest and understand the cyberspace threat.

Cyber attacks and strategies are difficult to understand, particularly from a decision-maker perspective.

This thesis will look at what a cyber wargame is, and how it can address the understanding of cyberspace operations through wargaming literature, previous cyber

[7] Matherly.
[8] Goldman, "Shodan."

wargames available or played through, expert interviews, and designer considerations. It will end with the limitations of cyber wargames and suggestions for the future of the discipline going forward.

Cyber warfare is a relatively new concept given the rise of the internet and the rapid interconnectivity of the physical world through, and to, the virtual. There are five key characteristics of cyber warfare that showcase how cyber wargaming is a useful tool for education and analysis.

Cyber warfare is new and dynamic.

The line between what is "theoretically possible with what is practically feasible" is not known in cyberspace.[9] There is constantly new malware and viruses emerging, like INCONTROLLER, a new toolset discovered in April 2022 that presents "an exceptionally rare and dangerous cyberattack capability."[10] The Russia-Ukraine cyber warfare has showcased unexpected thwarts or uses of technology. Civilian smartphones and apps were "used for the first time in military history as weapons powerful in their own way as rockets and artillery."[11] The government shifted Diaa, a government portal app for digital documents that functioned like a driver's license and linked users to virus vaccinations and permits, to also allowing citizens to report Russian soldiers' last

---

[9] Lennart Maschmeyer, "Why Cyber War Is Subversive, and How That Limits Its Strategic Value," War on the Rocks, November 17, 2021, https://warontherocks.com/2021/11/why-cyber-war-is-subversive-and-how-that-limits-its-strategic-value/.

[10] Claudia Glover, "New Malware Could Allow 'low-Skill' Hackers to Disrupt Critical Infrastructure," *Tech Monitor* (blog), April 14, 2022, https://techmonitor.ai/technology/cybersecurity/incontroller-malware-critical-national-infrastructure.

[11] Tim Judah, "How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders," *Financial Times*, April 10, 2022, https://www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8.

observed location.[12] Ukrainian intelligence aggregates the data on a map to inform their planning. There is a chatbot, eVorog, available on the Telegram app that links citizen messages to the Ukraine military, while information from Viber, another messaging app, led to artillery fire against Russian soldiers.[13] Ukrainian forces hid from thermal imaging drones by holding pieces of foam mat over their heads to avoid showing up as heat spots.[14]

All of these are new and dynamic uses of technology and cyber tools. However, it is near impossible to pre-emptively predict these uses; trying to capture the next effect of cyberspace requires speculative and creative thinking. Cyber wargames offer an arena to examine and speculate new devices, toolkits, or technology-enabled methods that impact civilian or military infrastructure by modeling real or future scenarios and seeing how **cyberspace could develop.**

Cyber capabilities and attacks are covert and classified.

Cyber capabilities are heavily classified, particularly whenever technical details are discussed.[15] The advantage of cyber-superiority lies in secrecy. Cyber operations are, in part, an "intelligence contest," which Rovner defines with five elements:

---

[12] Drew Harwell, "Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War," *Washington Post*, March 24, 2022, https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/.
[13] Harwell; Yaroslav Trofimov, "A Ukrainian Town Deals Russia One of the War's Most Decisive Routs," *WSJ*, March 16, 2022, sec. World, https://www.wsj.com/articles/ukraine-russia-voznesensk-town-battle-11647444734.
[14] Judah, "How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders."
[15] Elizabeth Bartels, Interview with Elizabeth Bartel, November 23, 2022; Tom Mouat, Interview with Major Tom Mouat, Online Interview, February 7, 2022.

> "First, it is a race among adversaries to collect more and better information. Second, it is a race to exploit that information to improve one's relative position. Third, it is a reciprocal effort to covertly undermine adversary morale, institutions, and alliances. Fourth, it is a contest to disable adversary capabilities through sabotage. Fifth, it is a campaign to preposition assets for intelligence collection in the event of a military conflict."[16]

Cyber operations are used for information theft, sabotage, disablement, or degradation of adversarial infrastructure, or to gain access for these purposes. All of the aforementioned elements apply to cyber capabilities, which are more successful when they are unknown. If your adversary does not know you can intrude on their network, they will place fewer resources on trying to pre-emptively defend their network or on trying to discover your own capabilities. Therefore, it is against a country or organization's interest to publicly display what cyber capabilities it has, or to what extent those capabilities are effective, even among its allies. Even reports on cyber capabilities are ultimately unverifiable unless the country 'proves' it by running an operation that is discovered. Welburn, Grana, and Schwindt conceptualize this attacker-defender relationship as constant uncertainty, where the attacker and defender both are unaware of each other's true offensive, retaliatory, or defensive capabilities.[17]

---

[16] Joshua r, "Cyber War as an Intelligence Contest," War on the Rocks, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.
[17] Jonathan William Welburn, Justin Grana, and Karen Schwindt, "Cyber Deterrence or: How We Learned to Stop Worrying and Love the Signal," September 4, 2019, https://www.rand.org/pubs/working_papers/WR1294.html.

Cyber tools face the complications of 'perishability' and 'obsolescence.'[18] The former describes when a cyber weapon loses utility after its use because the defender patches the vulnerability, and the latter describes when a cyber weapon becomes obsolete even before usage because the defender pre-emptively fixes its system. [19] These updates that render cyber weapons useless happen naturally in cybersecurity, but they can be hastened with information on an adversary's cyber toolkit. The exact capabilities – both in regards to the technical means and effect – are kept under wraps. During the earlier months of the Russian invasion of Ukraine, President Biden was presented with proposals for the unprecedented usage of cyberweapons. The options ranged from shutting down internet, electricity, or disrupting the train systems for resupply lines – and while options varied, so did their impact, a source stated: "You could do everything from slow the trains down to have them fall off the tracks."[20] However, after this publication from NBC News, a spokesperson for the National Security Council stated that "This report is wildly off base and does not reflect what is actually being discussed in any shape and form."[21] Even for known cyber attacks, states will often choose to remain deliberately ambiguous on their involvement because it allows them to "manipulate rivals' perceptions of its cyber capability and resolve."[22] While this is not the sole reason, the covertness of cyber

---

[18] Christopher Bartos, "Cyber Weapons Are Not Created Equal," *Proceedings* 142, no. 6 (June 1, 2016), https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal.
[19] Bartos.
[20] Courtney Kube and Ken Dilanian, "Biden given Options for Unprecedented Cyberattacks against Russia," NBC News, February 24, 2022, https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.
[21] Kube and Dilanian.
[22] Joseph M. Brown and Tanisha M. Fazal, "#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations," *European Journal of*

warfare means that no state or person has a clear picture of what is happening or has happened. At best, without confirmation, it is an educated guess. For instance, the Mumbai blackout in October 2020 occurred a few months after the Chinese-Indian border skirmish, and while Recorded Future, a U.S. cyber company, found that Chinese malware was in the Indian electric control systems, and Indian officials at the time claimed that it was a Chinese-origin cyberattack, China has denied involvement.[23] This means, for a decision-maker, that there is no broad overview or baseline to work from regarding an adversary's, or sometimes even their own country's, cyber capabilities. Brown and Fazal note that "the first evidence of a cyber capability may be the active use of that capability in conflict," however, "states have incentives to maintain secrecy around these weapons so that their opponents do not develop countermeasures against them."[24]

Therefore, wargaming can help by creating a set of hypothetical capabilities, using open-source information, that can grant an idea of how the United States could operate within peacetime or conflict *if* it had these hypothetical resources and powers. Decision-makers can use this set of hypotheticals to inform current and future actions, and receive expert guidance on how one set of capabilities versus another would play out.

Cyber attacks are technical.

Cyber attacks are technical, and therefore the explanation of how cyber attacks work or what they will do within a system can be highly technical as well, particularly to

---

International Security 6, no. 4 (November 2021): 401–17, https://doi.org/10.1017/eis.2021.18.

[23] David E. Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, February 28, 2021, sec. U.S., https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

[24] Brown and Fazal, "#SorryNotSorry."

a non-expert audience. For instance, the most known and common cyber attacks are: "denial of service, logical bomb, abuse tools, sniffer, trojan horse, virus, worm, send spam, and botnet" but how these work with different systems, bypassing defenses, cannot be so easily summarized.[25] This makes for a difficult translation between what cyber experts do on a tactical level, network intrusions, and defense, to the higher levels of decision-making which is concerned about the effects and success probability.

Wargames can act as a translation mechanism, to bring together the cyber experts and the decision-makers, or operators of kinetic systems and cybersecurity, so the two can understand under a hypothetical situation how to cooperate and communicate with each other.

Cyber capabilities cannot be 'tested.'

Even if a decision-maker has the highest level of clearance, and they have experts translating the level of technical detail into real-world impact, there is no guarantee a cyber attack will succeed or have the intended effect. While the difficulty in testing military forces and power is not a new concept – you don't know if your forces are capable of beating another force unless you start a war, cyber weapons are semi-unique in that even 'known' capabilities are not confirmed to work.

There is no confirmation that secret capabilities would actually be successful. Nitro Zeus was the U.S.'s backup plan to Stuxnet, which allegedly would have allowed the U.S. to disable Iran's command and control systems, air defenses, power, financial

[25] Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7 (November 1, 2021): 8176–86, https://doi.org/10.1016/j.egyr.2021.08.126.

systems, and other major infrastructure.[26] The plan was shelved after the US-Iran nuclear deal. However, there was no guarantee that Nitro Zeus or any attempt for a state government to hack into another state's C2 systems would work; an insider to Nitro Zeus told the New York Times that "before it was developed, the US had never assembled a combined cyber and kinetic attack plan on this scale."[27] Even with investments of tens of millions of dollars, there is no guarantee that offensive or defensive cyber capabilities will be successful when the time comes.

Some methods attempt to test cyber weapons and defenses, such as penetration testing, which can check on a software system's security challenges by having cyber experts play the role of an external attacker, which has been used by the Department of Defense for years.[28] This relies on live exploitation of a system, but it has limitations because pseudo-attackers could miss a vulnerability, or, if trying to 'test' capabilities against an adversary, this requires the model of an adversary's network to be accurate.

Instead, wargames can create a 'range' of plausible outcomes, and then adjudicate or rely on probability rolls to see whether or not cyber operations succeed in one particular instance and the consequences of that success or failure.[29] Even if the probability of success or failure of a particular tool is inaccurate, it still allows for the

---

[26] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16, 2016, sec. World, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.
[27] Sanger and Mazzetti.
[28] Edward Hunt, "US Government Computer Penetration Programs and the Implications for Cyberwar," *IEEE Annals of the History of Computing* 34, no. 3 (July 2012): 4–21, https://doi.org/10.1109/MAHC.2011.82.
[29] Don Marrin, Jason Vogt, and Peter Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino, March 18, 2022.

human decision-making on what to do in response to the consequences of choosing to attack or defend.

There are no defined strategies or understood dynamics within cyberspace.

Cyber warfare is still relatively untested; there are no thresholds or norms. Unlike conventional warfare, where certain actions are generally understood to be provocative or to signal an intent to escalate and attack, cyber attacks, even when discovered, do not have the same guidelines. Fischerkeller and Harknett attempt to conceptualize 'agreed competition,' where "behaviorally, cyber actors appear to have tacitly agreed on lower and upper bounds of the cyber strategic competitive space."[30] However, this boundary is being tested constantly as attacks on critical infrastructure become more severe and frequent. Even cyber policy experts disagree on the purpose of cyber warfare during a conflict. For instance, the 2022 Russia-Ukraine conflict had many experts predicting a level of cyber conflict and damage that was not, as of April 2022, seen.[31] Some cyber experts believe that cyber attacks will not be a decisive factor in warfare, and others note that cyber exists "within grey zone conflict: the space between peace and war," "once bombs are being dropped, the primary goal for cyber operations comes in supporting conventional operations."[32]

---

[30] Michael Fischerkeller and Richard Harknett, "What Is Agreed Competition in Cyberspace?," Lawfare, February 19, 2019, https://www.lawfareblog.com/what-agreed-competition-cyberspace.

[31] David Cattler and Daniel Black, "The Myth of the Missing Cyberwar," April 13, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.

[32] Dmitri Alperovitch, "One Reason Why We Are Not Seeing Much Cyber Activity in Ukraine Right Now: Cyber Is a Perfect Weapon for Grey Zone Conflict: The Space between Peace and War. Once War Breaks out, Cyber Becomes Much Less Useful for Anything but Very Tactical Objectives in Support of Kinetic Ops," Twitter, March 2, 2022, https://twitter.com/dalperovitch/status/1499136582770733061?s=21; Jacquelyn Schneider, "This Is Exactly What I Found in Wargames--Once Bombs Are Being

If cyberspace attacks had norms or hard-drawn red lines, wargames could serve the purpose of seeing the action-reaction cycle according to anticipated adversary responses to certain actions. However, because cyberspace does not have norms, wargames can look at cyber escalation and crisis dynamics. By granting the 'plausibility' range of outcomes, decision-makers can practice responding to a variety of situations because there is no guarantee on which situation will occur in real life.

Dropped, the Primary Role for Cyber Operations Comes in Supporting Conventional Operations . . . but This Is Tactically Very Difficult Because Networks Are Changing," Twitter, March 2, 2022, https://twitter.com/jackiegschneid/status/1499137881205403650?s=21.

Chapter 2. What is a Cyber Wargame?

What is a wargame?

Wargaming is about war, but more importantly, it is about human decision-making.[33] There is no agreed-upon definition of what a wargame is, what types of wargames there are, or what a wargame is supposed to, or can do.[34] There are several definitions within the wargame community that have attempted to encapsulate what a wargame entails or is composed of, but they all caveat that this is an imperfect and shifting definition. Peter Perla, the author of "The Art of Wargaming" and a leading expert in wargaming, states that "what wargaming is not is often even less obvious than what it is."[35]

Therefore, this section will address attempted definitions of wargaming by looking at descriptions of what it is, its purpose, and its key characteristics.

---

[33] The definition of wargaming has begun expanding beyond 'war' and 'conflict as well, with some wargamers using wargame as an umbrella term. Bartels, Interview with Elizabeth Bartel.

[34] I had the opportunity to speak with 18 experts in wargaming, and across the board, each had their own definition of what wargaming is defined as and what it can be used for. Bartels; Jennifer McCardle, Interview with Jennifer McCardle, December 6, 2021; John Curry, Interview with John Curry, February 2, 2022; Mouat, Interview with Major Tom Mouat; Reid Pauly, Interview with Reid Pauly, February 16, 2022; Kate Lea, Interview with Kate Lea, March 2, 2022; Frank Smith, Interview with Frank Smith, March 9, 2022; Erik Lin-Greenberg, Interview with Erik Lin-Greenberg, March 11, 2022; Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino; Yuna Wong, Interview with Yuna Wong, February 19, 2022; Andrew Haggman, Interview with Andrew Haggman, March 24, 2022; Jeremy Sepinsky, Interview with Jeremy Sepinsky, March 28, 2022; Elçin Ada SAYIN, Interview with Elçin Ada SAYIN, April 13, 2022; Sebastian Bae, Interview with Sebastian Bae, April 22, 2022; Brandon Valeriano, Interview with Brandon Valeriano, April 22, 2022.

[35] Peter P. Perla, "What Wargaming Is and Is Not," *Naval War College Review* 38, no. 5 (1985): 70.

While Perla warns away from writing a single definition, he provides one of the most cited and accepted definitions: "a wargame is an exercise in human interaction… the exploration of the role and the potential effects of human decision."[36] Many in the community have attempted to combine and address his 1990 definition, and a useful, more extended definition of wargaming that acts as a baseline is:

> "Adversarial by nature, wargaming is a representation of military activities, using rules, data, and procedures, not involving actual military forces, and in which the flow of events is affected by, and in turn affects, decisions made during the course of those events by players acting for all actors, factions, factors, and frictions relevant to those military actions."[37]

Jeremy Sepinsky, CNA's lead wargame designer, has a definition of wargaming as:

> "Wargaming is creating a structural process to compile and organize disparate sets of information. My style of wargaming, my method of design, is all about understanding how people as unique actors within the space of a challenging problem are going to react to different stimuli and what information is required to achieve the desired end state. Wargaming is not about war, it is about designing a process to answer a question."[38]

In Haggman's Ph.D. thesis on cyber wargaming, he proposes his own definition for the use of wargame, as a method to "understand events of the past, plan operations

---

[36] Peter Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Annapolis, MD: Naval Institute Press, 1990), 164.
[37] Graham Longley-Brown, "What Is Wargaming? | LBS," 2015, http://lbsconsultancy.co.uk/our-approach/what-is-it/.
[38] Sepinsky, Interview with Jeremy Sepinsky.

and organizations for the present, and explore envisaged futures."[39] The last purpose is broken down further into imagining futures, actioning futures – generating lessons that can be applicable, anticipating futures – creating future effects in order to react to them or modeling, and preventing or enabling futures.[40]

Lin-Greenberg, Pauly, and Schneider in "Wargaming for International Relations Research" apply their definition through features: "wargames are interactive events that display four characteristics: human players, immersed in scenarios, bounded by rules, and motivated by consequence-based outcomes."[41] Another definition based on elements is from Graham Longley-Brown, another frequently cited wargamer and author of "Successful Professional Wargames: A Practitioner's Handbook,": the three key elements are players, decisions, and adversarial content.[42] This breaks down into seven general building blocks: "aim and objectives, scenario, players, databases, models/simulations, rules, procedures and umpires, and analysis."[43] The Joint Planning report lists that effective wargaming involves: (1) a well-developed, valid COA (Course of Action), (2) people making decisions, (3) a fair competitive environment, (4) adjudication, (5) consequences of actions, and (6) iteration."[44] Bartels writes that games have five key aspects: (1) objectives, (2) environment for context, (3) player roles, (4) rules that define

---

[39] Andreas Haggman, "Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education" (PhD Thesis, Royal Holloway, University of London, 2019), 25–27.
[40] Haggman, 26–31.
[41] Erik Lin-Greenberg, Reid B.C. Pauly, and Jacquelyn G. Schneider, "Wargaming for International Relations Research," *European Journal of International Relations*, December 17, 2021, 3, https://doi.org/10.1177/13540661211064090.
[42] Longley-Brown, "What Is Wargaming? | LBS."
[43] Longley-Brown.
[44] Joint Publication 5-0, "Joint Planning" (Washington, DC: The Joint Staff, December 1, 2020), III-27.

how to make decisions and the consequences of those decisions, and (5) analysis that converts the lessons from the game into knowledge.[45]

The ultimate question is: what makes for a *successful* wargame. The unsatisfying, but accurate, answer is that it very much depends on the wargame itself. "Next-Generation Wargaming for the U.S. Marine Corps" includes a section that defines the criteria a wargame needs to be successful: have relevant results in a reasonable timeline for the study, inform decision making, identify lessons for the future, ensure decision-makers are aware of the game's utility, benefits, and limitations, participants should feel camaraderie, and the game should be fun.[46] However, these criteria feel too broad and expansive to judge a wargame on, for instance, an educational wargame may not necessarily need to have relevant results, or an analytical game may not require that participants feel camaraderie.

In multiple interviews with experts, questions regarding game methodology and success were met with the answer: It depends on what the purpose of the game is. [47] A successful wargame fulfills its purpose; a good wargame design leads to the purpose of

---

[45] Elizabeth Bartels, "Innovative Education: Gaming - Learning at Play," *ORMS Today* 41, no. 4 (August 2014), https://pubsonline.informs.org/do/10.1287/orms.2014.04.13/full/.

[46] Yuna Wong et al., "Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action" (Santa Monica, CA: RAND, 2019), 93.

[47] This answer was consistent across the board with every expert interview. Bartels, Interview with Elizabeth Bartel; McCardle, Interview with Jennifer McCardle; Curry, Interview with John Curry; Mouat, Interview with Major Tom Mouat; Pauly, Interview with Reid Pauly; Lea, Interview with Kate Lea; Smith, Interview with Frank Smith; Lin-Greenberg, Interview with Erik Lin-Greenberg; Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino; Wong, Interview with Yuna Wong; Haggman, Interview with Andrew Haggman; Sepinsky, Interview with Jeremy Sepinsky; SAYIN, Interview with Elçin Ada SAYIN; Bae, Interview with Sebastian Bae; Valeriano, Interview with Brandon Valeriano.

the wargame being accomplished. Anything else in the wargame that does not directly relate to its intended outcome is "window dressing".[48]

What is a cyber wargame?

A cyber wargame follows the same vein as a normal wargame, except, as suggested by the name, it incorporates the domain of cyberspace and/or advanced technology. A useful distinction for cyber wargames is whether it is a 'cyber wargame' or a 'cyber-in-game.'[49] As implied by the name, a cyber wargame analyzes a cyber problem, whether that is in 'cyberspace' or the effects/impact/development of a certain technology. Whereas a cyber-in-game wargame is one where cyber operates as an enabler; the main purpose of the game is on combat itself. The question is, is the game about combat and the effects that cyber can have, or is it a game for 'cyber' experts, in which case the combat is the background and the focus is on managing cyber capabilities and actions.[50] The following are the elements of a cyber wargame: the sponsors, designers, purpose, participants, game format, scenario, representation of cyber capabilities, adjudication, and data generated.

Sponsor

The sponsors for cyber wargames determine the purpose of a wargame. From the government side, the sponsors are often military-based, from the Navy, Airforce, etc. Generally, the sponsor's original request will come from a higher level but the main

---

[48] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.

[49] This information comes from an interview with an unnamed source, who agreed to speak without attribution – but is considered an expert in the wargaming field. Interview with Unnamed Source, February 19, 2022; Ed McGrady, Interview with Ed McGrady, February 18, 2022.

[50] Interview with Unnamed Source.

interaction will be with an officer; CNA typically works with officers at the O6 or higher level.[51] Officers will typically not be well-versed in wargaming, which has been treated both as an area of improvement and a non-concern by different designers.

Designers

While there are 'in-house' designers, for instance, the Cybersecurity and Infrastructure Security Agency have designers that create their own games and scenarios, oftentimes, games are outsourced or made in collaboration with contractors or federally funded research and development centers (FFRDCs). A few companies that work on wargaming include: Booz Allen Hamilton, Deloitte, Leidos, BAE Systems, General Dynamics; FFRDCs include Institute for Defense Analyses (IDA) and Center for Naval Analyses (CNA), and there are a few thinktanks that also have a wargaming section, like the Center for New American Studies and the Hoover Institute.

Purpose

Each wargame will have a different 'ask' behind it, and different wargame designers have attempted to categorize the purpose of different games. The first deciding factor, and one of the few classifications that designers agree on, is whether or not the game is *educational* or *analytical.* The Connections Conference, a conference that brings together wargamers annually lists three applications: "decision-making, education and training, and recreation."[52] Analytical and education fit the first two applications, and the third is recreational or entertainment games – games built for fun. It is difficult to categorize these purposes into a purely educational or analytical function. Imagine, for

[51] Sepinsky, Interview with Jeremy Sepinsky.
[52] "Wargaming," *Connections Wargaming Conference* (blog), June 2, 2015, https://connections-wargaming.com/wargaming/.

instance, a game designed to integrate knowledge between experts that is meant to educate experts on the gaps in their own knowledge or teach people across corporations and the public sector how to cooperate, or generate data on how public-private sector individuals work together. That being said, games should have a primary focus of being educational or analytical (intended to teach or generate data), but many educational games can generate data for potential analysis (if collected), and analytical games can teach participants.

The value of both games is an ongoing debate within the wargaming community, but a basic distinction between the two is if the game is meant to generate new information for players or the sponsor. Bartels describes the difference as if the game is meant "to teach existing knowledge or to produce new knowledge."[53] However, note that analytical wargames are not predictive wargames; wargames do not have the power to predict what will happen in the future, but they can show plausible potential futures.[54] The purposes are roughly sorted into the conception of a purpose of a wargame from academia and government entities, however, note that the individual authors are not representative of their organizations, it only reflects their individual view.

Academia

In "Wise Choices: Decisions, Games, and Negotiations," published in 1996, Edward Parson, UCLA Law Professor, wrote that simulation gaming is for "informing complex, difficult, and high-stakes policy and decision problems" and proposes four models to

[53] Bartels, "INNOVATIVE EDUCATION."
[54] These interviews were conducted with wargame *designers and analysts,* not with wargame *sponsors.* Several expert designers have noted that sponsors can over-estimate the ability for

achieve this purpose.[55] These classifications have been cited numerous times since then as examples of purposes that wargames can serve.

(1) Experiments[56]: Experiments attempt to prove or disprove a hypothesis that can be generalized or abstracted to be applied more broadly. However, Parson notes that this can miss answering policy problems because of any unique aspects of the issue. Additionally, finding the right participants to test the hypothesis on will be difficult, because it requires finding either the people that would be answering those policy problems to simulate experiments that would replicate real-life or close-enough substitutes. The more complex and 'high-up' the problem, the more difficult; to create an experiment on whether or not the U.S. would use cyber weapons against Russia, for instance, it would be best to pull the U.S. President, barring that, to go down the line to find the person that understands the actions the President would take best, but is also available to participate in a wargame.

(2) Instruct Decision Makers[57]: Parson defines this in a very narrow way, simulations that want to specifically "instruct decision-makers in the essential character of a complex policy problem," which requires that the simulation be realistic enough to create useful learning regarding the issue. He references the changing definition of chemical understanding, for instance, that affected the understanding of global climate change.[58] Parson also takes issue with this method because he writes that

---

[55] Edward Parson, "What Can You Learn from a Game?," in *Wise Choices: Games, Decisions, and Negotations*, ed. R. Zeckhauser, R. Keeney, and J. Sevenius (Harvard Business School Press, 1966), 234.
[56] Parson, 237.
[57] Parson, 240.
[58] Parson, 241.

it is very difficult to achieve the realism required, particularly for changing policy issues.

(3) Promote Creativity and Insights[59]: These simulations have no defined ending or rules, instead, they are supposed to break out of habitual thinking. There are two requirements of these games, that the rules and structure are open to challenge and renegotiation during the game, and that a post-simulation debrief where actions, alternative actions, applicability, and generalization of knowledge are confirmed against the expert participant opinions outside the game.[60]

(4) Simulations for the Integration of Knowledge[61]: The purpose of these simulations is to bring together a group of experts and create a compiled knowledge database through the simulation mechanisms of an open design, forced use of knowledge through making decisions in the game, and the lived-through experience of applying the knowledge and seeing consequences within the game.

In Wargaming for International Relations, Lin-Greenberg, Pauly, and Schneider, explain how to use wargames as a research tool as an experimental wargame or an observational wargame. Experimental wargames look at "what is the effect of X on Y?" while observational wargames look at "How might decision-makers behave in a specific type of event? How might an event unfold?"[62] Observational wargames look at a possible outcome given a scenario, and therefore fit best for "general decision-making processes

[59] Parson, 241.
[60] Parson, 242.
[61] Parson, 246.
[62] Lin-Greenberg, Pauly, and Schneider, "Wargaming for International Relations Research."

or generating hypothesis" while experimental games test hypotheses via "treatment' and 'control'."[63]

Federally Funded Research and Development Centers (FFRDC)

In a RAND report from expert wargame designers with experience from a variety of FFRDCs, "Next Generation Wargaming for the U.S. Marine Corps, the authors lay out a framework of wargaming capabilities: "Concept development", "Capabilities development and analysis", "Science and technology wargaming", "Senior leader engagement and strategy discussion", "Operational decisions and plans", and "Training and Education."[64]

Rand Corporation

The RAND Corporation is a federally funded research development center that designs wargames for various U.S. military and defense sponsors. Their wargaming sector lists the purposes of wargames to "examine warfighting concepts, train and educate commanders and analysts, explore scenarios, and assess how force planning and posture choices affect campaign outcomes."[65]

Elizabeth Bartels is the co-director of the RAND Center for Gaming and is one of the top experts in wargaming. Her work has been centered on wargaming, and she has published extensively on the categorization of wargaming purposes and types.

---

[63] Lin-Greenberg, Pauly, and Schneider.
[64] Wong et al., "Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action."
[65] RAND, "Wargaming," accessed April 6, 2022, https://www.rand.org/topics/wargaming.html.

Bartels divides games into four categories: discovery, educational, analytical, and training games:[66]:

	Creating Knowledge	Conveying Knowledge
Unstructured Problem	Discovery Game: "Investigation of new problems, consideration of potential future conditions and rare events such as black swans" [67]	Educational Game: "Instruct participants about poorly structured phenomena" [68]
Structured Problem	Analytical Game: "Illustrate how human decisions interact with well-defined… phenomena" [69]	Training Game: "Train individuals about specific, well-understood tasks" [70]

In her Ph.D. dissertation, "Building Better Games for National Security Policy Analysis, Bartels focuses specifically on analytical games and creates four archetypes based on: "How mature is the research? Are you focused on understanding the nature of the problem or trying to understand the solution to that problem?"[71]

(1) "System exploration": Players and designers should understand a policy problem and its evolution. This game should result in a model of the problem that helps improve the sponsors' understanding of the issue, to try to develop a concept of the initial problem.

(2) "Alternative conditions": These games have comparative or experimental frameworks and attempt to identify decision-making patterns based on the context

[66] Bartels, "INNOVATIVE EDUCATION."
[67] Bartels.
[68] Bartels.
[69] Bartels.
[70] Bartels.
[71] Bartels, Interview with Elizabeth Bartel.

of the problem, the goal is to identify a causal connection. These games focus on how the decisions of players impact their environment.

(3) "Innovation": These games test outside the status quo to attempt to come up with new potential solutions for the future.

(4) "Evaluation": These games try to create a causal outcome from player actions to identify the pros and cons of a course of action. These games are centered around the consequences of player decision-making.

These archetypes are presented on a spectrum.[72] If the focus on the game is on the problem, the outcome is likely to be more descriptive, while if the focus is on a solution, the outcome is likely to be more prescriptive or recommendation-based. [73] System exploration games occur early on in research and look at the problem concept, alternative conditions occur during the middle and look at the decision-making process, innovation games occur during the same period and look at decisions themselves, and evaluation games occur during the later confirmation and refinement stages and look at the consequences of decisions. [74]

Center for Naval Analyses

CNA has five different purposes, provided in a three-step question model in a two-page brochure given to sponsors. The first question addresses the purpose of the game: "What is your organization's desired outcome as a result of the wargame? What do

[72] Elizabeth Bartels, "Building Better Games for National Security Policy Analysis," Dissertation (RAND Institute, March 2020), 63.
[73] Bartels, 65.
[74] Bartels, 66.

you want the wargame to enable your organization to do?" [75] The outcomes are: "Socialize a concept," "Explore an idea," "Refine a concept," Model a process," and "Educate the players." [76] This idea of exploring questions is re-iterated in interviews with CNA wargame designers, who note that "wargaming is not about forecasting what will happen, they are about identifying the possibilities and refining the questions that your audiences need to be asking."[77] While wargames are typically built around a problem set, they can also be used to understand whether the conceptualization of the problem set in the first place is accurate.

CNA follows a three-part model for analysis games, referred to as the cycle of research. They are explicit in noting that wargames do not exist in a vacuum, they cannot validate or prove a hypothesis on their own, nor can they predict.[78]

> "(1) Wargames discover questions for analysis to explore and recommendations that can be exercised.
>
> (2) Analysis develops theories that can be wargamed and suggests possibilities that can be exercised.
>
> (3) Exercises communicate the realities of warfare to analyze and present practical limitations to wargames"[79]

---

[75] CNA, "So You Want to Sponsor a Wargame..." (Center for Naval Analyses, n.d.), https://www.cna.org/centers/cna/operational-warfighting/wargaming.
[76] CNA.
[77] Lea, Interview with Kate Lea.
[78] Chris Steinzer, "We Should Never Say That a Wargame 'Proved' or 'Validated' Anything. Nor Should We Ever Expect Games to Be Predictive.," Twitter, April 5, 2022, https://twitter.com/SteinitzChris/status/1511340161002610697.
[79] CNA, "So You Want to Sponsor a Wargame..."

What Can A Cyber Wargame Do?

While the aforementioned purposes provide a general overview of how wargames can be used, cyber wargames, while fitting into this category, also offer some more nuanced purposes because they deal with cyberspace. Even the term analytical, although it will be used in this thesis, is contested. As Ed McGrady notes in "Getting the Story Right on Wargaming," "wargaming is not analysis… you can analyze wargames," but they generate "'dirty' data."[80] He claims that wargames are not rigorous experiments; their results cannot be replicated and the outcomes often differ game-to-game.[81] This is a differing opinion from an emerging area of research for wargames as experiments, which attempt to solve this problem via iteration or through designing games that can use 'dirty' data.[82]

Corresponding Purposes of Cyber Wargames: Analytical

The defined purposes of wargames from different institutions and experts overlap in some areas and diverge in others, but they can offer a framework for assessing the potential purposes of cyber wargames.

Explore a Cyber Concept

These games correspond with Bartel's purposes of system exploration, creating knowledge with an unstructured problem, the RAND reports' purposes of examining

[80] Ed McGrady, "Getting the Story Right about Wargaming," War on the Rocks, November 8, 2019, https://warontherocks.com/2019/11/getting-the-story-right-about-wargaming/.
[81] McGrady.
[82] Lin-Greenberg, Pauly, and Schneider, "Wargaming for International Relations Research."

warfighting concepts and concept development, and the Center for Naval Analyses' purpose of exploring an idea.

Explore the Understanding of Existing Cyber Policies

With the rise of cyberspace, there have also been several policies and concepts that are difficult to test without engaging in conflict or without a live event. For instance, the idea of "Defending Forward" and "Persistent Engagement" or concepts like cyber deterrence and cyber escalation could be run in a wargame simulating cyber conflict on an international level to materialize, in concrete terms, what these phrases entail.[83]

Explore Communications within a Cyber Context

Cyber attacks have the unique ability to shut down and manipulate communication channels, which is an issue that has received little attention within civilian critical infrastructure until recently. For trends in attacks like ransomware or increased denial of service, understanding the concept of limited, untrustworthy, or unreliable communications and how that impacts other aspects of normal operating procedures is crucial. Wargames that raise these vulnerabilities can help kickstart future research or plans into backup communication tools.

Understand How Cyber Operations Can Affect Kinetic Infrastructure

---

[83] David Vergun, "'Persistent Engagement' Strategy Paying Dividends, Cybercom General Says," U.S. Department of Defense, November 10, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2840284/persistent-engagement-strategy-paying-dividends-cybercom-general-says/; Aaron F. Brantly, "The Cyber Deterrence Problem," in *2018 10th International Conference on Cyber Conflict (CyCon)* (2018 10th International Conference on Cyber Conflict (CyCon), Tallinn: IEEE, 2018), 31–54, https://doi.org/10.23919/CYCON.2018.8405009; Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review*, September 28, 2020, https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

There is a growing concern regarding how interconnected and 'online' infrastructure is, like port systems and traffic systems. A wargame that looks at how cyber attacks shut down critical infrastructure and the analog effect on the real world can help with the conceptualization of private-public sector partnership or the need for policies that mandate federal reporting of criminal attacks on private institutions.

Develop or Test Cyber Plans or Plans with the Inclusion of Cyberspace

The purpose of these games corresponds with Bartels' purposes of innovation or alternative conditions, creating knowledge with a structured problem, the RAND reports' purposes of assessing how force planning and postures choices affect campaign outcomes, operational decisions and plans, and senior leader engagement and strategy discussion.

Test the Effectiveness of Current or Future Cyber Response Policies

There is no need for a cyber response plan until a cyber attack happens, but if a cyber attack happens and there is no cyber response plan, then response becomes incredibly difficult and confusing. The development and testing of cyber response plans can be run through wargames that create a realistic environment and threat, and bring together participants representing the existing organizations into one overarching crisis simulation. This can be done both for civilian and national-level plans, such as what is done when there is a large-scale ransomware attack across multiple sectors, or for military conflicts at any level, such as an electromagnetic pulse that shuts off intelligence, surveillance, and reconnaissance capabilities.

Assess the Integration of Cyber Warfare into Multi-Domain Conflict

Games that look at integrating cyber plans into existing conflict, such as simulations regarding hybrid warfare, are useful because they show the creative or predictable ways that cyber attacks add to warfare. For instance, a cyber wargame that throws in social media influence campaigns on top of a conventional warfare conflict, or a wargame that allows weapons systems to be disabled or degraded through cyber means without needing the resources to destroy the systems in the real world.

Identify Potential Failures or Weak Points: Winners Win, Losers Learn (and Change)

In October 2020, the Pentagon wargamed a battle for Taiwan as a "test for a new Joint Warfighting Concept" which was based on previous warfighting concepts.[84] The blue team lost network access at the onset of the game, overturning assumed access to information, and the aggregation of forces to support combat power made forces more vulnerable because of their combined location. After the results of this wargame, a miserable loss, the U.S. introduced a new concept, "Expanded Maneuver," in hopes of addressing old assumptions regarding information networks, logistics, and positioning. Games that try, specifically, to identify points of failure due to cyber warfare within military operations or peacetime infrastructure functioning could help change within a system.

Assess Cyber-Related Decision-Making Through Experiments

These games correspond with Bartels' purpose of alternative conditions, Lin-Greenberg, et al.'s experimental wargames, and Parson's experimental wargames. These

[84] Tara Copp, "'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight," Defense One, July 26, 2021, https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/.

games will typically have a control and a treatment group or will attempt to manipulate the environment in some way to assess the response and create a causal relationship between an environmental effect and the player's response, or vice versa.

How Decision-Makers Will Respond to Cyber Attacks of Varying Levels

While it is difficult to prove or disprove a hypothesis, in regards to what will actually happen if a certain cyberspace operation is launched, wargames do offer a way of testing hypotheses regarding the perception of cyber operations. Social science research that utilizes surveys and randomized, controlled experiments could expand from scenarios into fully-fleshed out wargames testing the human decision-making response in a cyber scenario. This would also increase the ecological validity (whether or not the study can be generalized to the real world) of the experiment by creating more realistic environments for the participants. For example, a 2021 study tested asked if "exposure to cyber terrorism prompt calls for retaliatory military strikes" by exposing participants to cyber and conventional terrorist attacks on critical infrastructure through television news reports.[85] While the study found that "only lethal cyber terrorism triggers strong support for retaliation", placing this in a wargame setting where participants would have to 'see' the consequences of their retaliation through gameplay could alter the findings.[86] Using wargames as experiments is seen in the International Crisis Wargame, which tests four

[85] Ryan Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment," *British Journal of Political Science* 52, no. 2 (February 2021): 850–68, https://doi.org/10.1017/S0007123420000812.
[86] Shandler et al.

hypotheses on nuclear usage with the inclusion of cyber operations through using experimental design.[87]

Assess How Conflict Could Arise, Motivated by Cyber Attacks

Similar to the previous purpose, games could also test how the action-reaction cycle of cyber escalation can snowball. By placing red and blue teams with motivations for conflict, sponsors can attempt to trace the different paths that cyber could escalate a conflict. In 2011, the Guardian reported that the United States and China ran two war games "that were designed to help prevent a sudden military escalation between the sides if either felt they were being targeted," organized by the Centre for Strategic and International Studies (CSIS), a D.C. thinktank, and the China Institute of Contemporary International Relations, a Beijing thinktank.[88] While running wargames with adversaries is unrealistic, for one, and would be unlikely to generate any useful data due to an unwillingness to signal intentions, for two, a similar wargame that models US-China or US-Russia conflict with experts playing as the red team could see how cyber attacks could create a conflict.

Speculate on Future Technology Capabilities and Scenarios

The purpose of these games corresponds with Bartels' purposes of creating knowledge with an unstructured problem, the RAND reports' purposes of exploring

---

[87] Benjamin Schechter, Jacquelyn Schneider, and Rachael Shaffer, "Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming," *Simulation & Gaming* 52, no. 4 (August 1, 2021): 513–26, https://doi.org/10.1177/1046878120987581.

[88] Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, https://www.theguardian.com/technology/2012/apr/16/us-china-cyber-war-games.

scenarios, capabilities development and analysis, and science and technology wargaming, and Parson's purpose of promoting creativity and understanding.

Speculate on Future Cyber Scenarios

Although experts have speculated on what a total cyber-catastrophe or critical points of failure could look like, the ultimate issue is that no one understands cyber the same way that we understand what nuclear war and fall-out could look like. Wargames built around looking forward into worst-case scenarios or how technologically advanced warfare could be are useful for trying to future-plan. For instance, a game that models what cyber conflict in a certain region could entail, or what a cyber black swan event would look like.

Extend Capabilities through Technology

In the same vein, even though it can be near-impossible to predict the next generation of technology or the next game-changer, games can look at how technology can extend capabilities. A game that posits: what if there is a technology that allows for total surveillance, or quantum transfer of information at impossible levels of encryption or unbelievably fast speeds. For simulations like these, the actual technology is not important, instead, it is the effect of extending capabilities beyond the realm of current possibility and how decision-making would be impacted if players suddenly had to deal with the development of a technology that has no counter or overturns conventional assumptions.

Refine Cyber Response Plans

The purpose of these games corresponds with Bartel's purpose of evaluation and the Center for Naval Analyses' purpose of refining a concept.

These games are about testing the refinement of a pre-existing plan after it has gone through change. For instance, if a government has developed a cyber response plan, it can run a large-scale wargame to check the future drafts of this plan and attempt to discover and mitigate weaknesses in design or execution. This purpose overlaps with the testing of cyber response plans but is more focused on whether or not updates to an original model are useful.

Corresponding Purposes: Educational

Education, exercise, and training: Bartels' purposes of conveying knowledge with an unstructured or structured problem, CNA's purpose of socializing a concept, educating players, and modeling a process, Parson's purpose of instructing decision-makers in understanding a problem and integration of knowledge, and the RAND reports' purposes of training, education, and educating are all under the same umbrella. Any of the above game concepts could also serve as an educational game, where the knowledge is primarily centered on the learning of the players within the game.

Exercise a Cyber Response Plan with a Cyber Attack Scenario

These games correspond with the Center for Naval Analyses' purpose of modeling a process. Governments and agencies will develop cyber response plans but will need to test them out to make sure participants understand their roles and responsibilities. Rather than waiting for an attack to occur, a wargame can ensure players have live practice with implementing a response and coordinating with others in the case of a worst-case scenario, such as an attack that shuts down communications or disables critical infrastructure.

Act as a Communication Tool Between Cyber and Non-Cyber Experts

The purpose of these games corresponds with Parson's purpose of integration of knowledge. Cyber experts and non-cyber experts can use the wargame as a platform to communicate technical concepts into policy and vice versa; understanding how cyberspace operations affect the analog world and vice versa. Wargame design can place a limit on the level of technical detail or ask cyber experts to explain effects to decision-makers, and decision-makers can learn how to ask for certain solutions based on realistic cyberspace capabilities.

Teach Non-Experts Cyber Concepts

Wargames can act as a hands-on method for the education of cyber concepts, such as how hacking works generally, or the delivery of various malware and viruses.

While this list has several generalized purposes for cyber wargames, this is in no way all-encompassing or inclusive. Instead, this record acts as potential ways cyber wargames fit into pre-existing concepts of the purpose of wargames, and there will be cyber wargames that do not fall into any of these categories or fit several at once.

Participants

The players for a cyber wargame are listed as the second-most crucial aspect of wargaming, even before the actual design of the game.[89] Because wargames are, at their core, about *decision-making,* wargame participants should be the people that would be actually making the decisions (or simulate a similar mindset) for both analytical games (to analyze realistic results) or for educational games (so participants can apply their

[89] Interview with Unnamed Source; Bartels, Interview with Elizabeth Bartel.

learned knowledge). If human decision-making is not a core component of the wargame, then the question can likely be answered through another method, like a study or detailed analysis.[90] The participants and purpose will also define the game structure by helping set out who is playing what. Bartels writes that there are three common roles in educational games, roles that are designed to educate the player in (1) how their real-life role fits into a scenario, (2) how a future role they may hold works, or (3) how someone else's role works (i.e. red teaming).[91]

It can be difficult to get the right people into the room, particularly for cyber games. Cyber experts for highly technical games are in high demand, and participant draw may rely on personal connections – the ability to pick up the phone and say, "Hey, we're running a game in two weeks, can you send over people matching this set of qualifications." And, oftentimes, the people who get sent are the youngest on the ladder because they have the most time. However, the right player or an expert player does not mean a 'wargamer.' In fact, often it may be preferential to have non-wargamer subject matter experts: participants who will try to win by relying on their real-world expertise rather than potentially by trying to break the game or find the loopholes.[92] Players are there to provide subject matter within the context of a particular problem, they are not there to win the game.

> "I design a wargame to answer a question, but the players are not there to answer that question. The players are there to answer specific questions within the context of the wargame, which creates information to pass on to other people in

[90] Sepinsky, Interview with Jeremy Sepinsky.
[91] Bartels, "INNOVATIVE EDUCATION."
[92] Sepinsky, Interview with Jeremy Sepinsky.

the wargame, which they combine to move the state of the game forward and the progression of the state of the game within that context answers the question that the game began with."[93]

Game Format

The format of a wargame can determine whether or not it is considered a wargame. For instance, the Naval War College distinguishes what is not automatically considered a war game: an exercise may be considered a wargame, a seminar and a seminar game are not the same, a workshop has a specific output, an experiment is more rigidly structured with a hypothesis, controls, and repetition.[94] Cyber exercises have been broken down into three different categories: table-top exercises, hybrid exercises, and live exercises.[95] One debate, for instance, is whether 'live hacking exercises' or 'red-teaming' should be classified under wargames or exercises. Exercises typically encompass a much broader category, where 'live' computer hacking or 'in-person' military drills can fall under this definition. "Live hacking" is not wargaming because it is not an abstract representation of conflict, and therefore will not be included in the analysis section of other cyber wargames. Connections Wargaming Conference, the annual wargaming conference that is regionally based (Connections US, Connections UK, etc.), lists four types of wargames: "constructive [abstract representations of forces], live, virtual, and multitype." [96] The Center for Naval Analyses breaks down wargaming

[93] Sepinsky.
[94] Us Naval War College, "About Wargaming," accessed March 9, 2022, https://usnwc.edu/Research-and-Wargaming/Wargaming/About-Wargaming.
[95] Jason Kick, "Cyber Exercise Playbook" (The MITRE Corporation, 2014).
[96] "Wargaming."

into four different classifications: “Force-on-Force Operational” (classic team wargames), “Operational Troop-to-Task” (resource management, specific to an organization’s staff and structure), “Event-driven Decision Support” (for early potential action or concept planning) and “Seminar-Style” (more on the exchange of ideas, typically for subject matter experts to generate ideas).[97]

In an interview with Major Tom Mouat, Directing Staff Office for Simulation and Modelling in the Technology Division at the Defense Academy in the United Kingdom, he lists three categories of cyber wargames.[98] There are “Re-skinned” games that have cyber capabilities slapped on top of them; Mouat is most critical of this category because it is not built to explore the aspects of cyberspace and therefore not useful for education. There are Choose-Your-Own-Adventure games where capabilities and choices are pre-determined and laid out.[99] He references a game designed within DSTL that follows this format, and he finds procedural path style games to be a useful teaching tool. Lastly, there are matrix-style games, which are heavily open-ended and reliant upon the adjudication. These are often stopped before a full-blown victory is reached on one side or another to shape analysis of the game without too much influence or focus on the ‘winners’ and ‘losers’ of the wargame.

---

[97] CNA, “Wargaming | CNA,” accessed November 30, 2021, https://www.cna.org/centers/cna/operational-warfighting/wargaming.
[98] Mouat, Interview with Major Tom Mouat.
[99] Specifically, Mouat cited the “Fighting Fantasy” gamebook series in the United Kingdom, more commonly known in the United States as Choose-Your-Own Adventure books.

In "The Handbook of Cyber Wargames," Curry and Drage break down cyber wargames into broad categories: penetration testing, seminar games, interactive cyber wargames, and analytical cyber wargames.[100]

(A) Penetration testing or red teaming: A cyber-attack is launched against the organization as a test of its current infrastructure and defenses.[101] Penetration testing, although not necessarily considered a wargame, has been incorporated into several as a 'live-fire exercise.' For instance, Locked Shields, the annual international live-fire cyber war game played between NATO countries creates a virtual fictional scenario where the red team utilizes penetration testing to attempt to compromise IT systems within the game.[102] However, this thesis will disregard penetration testing or red teaming because it does not deal with the wargaming concerns of 'abstraction' and 'representation' and instead has its own complications of designing an adequate, technical hacking challenge.

(B) BOGSAT (Bunch of Guys Sat Around a Table): Seminar games or 'free kriegsspiels' games where scenarios are played out and arbitrated by a games master. There are three levels of this type of gaming:

   a. The Train Station – A game style with a series of 'stops' that progress regardless of the players' actions.
   b. Choose-Your-Own-Adventure – Similar to the book series, there is no one determined ending, but players are still limited by a series of choices.

---

[100] John Curry and Nick Drage, *The Handbook of Cyber Wargames: Wargaming the 21st Century*, 2020.
[101] Curry and Drage, 3–4.
[102] Nic Hall, "2d TSB Cybersecurity Division at the Forefront of the World's Largest Live-Fire Cyber Exercise," *U.S. Army*, August 14, 2018.

c. Active Opponent – A red team counters the blue team's actions. Curry and Drage cite matrix games as an example of an active opponent style game – BOGSAT seminars where adversarial teams argue for what the outcome should be and often use a random number generator to determine the probability and outcome.[103]

(C) Interactive Cyber Wargames: Games focus on realism and live practice with no defined ending, but require a lot of adjudicators, are subject to derailment due to a flexible ending and have an increasing difficulty in coordination as the scale of the game grows.[104]

(D) Analytical Cyber Wargames: Games designed to analyze situations, rather than educate participants.[105]

Scenario

The scenario describes the setting, background, and conflict justification of the game.

Is the conflict in the scenario played out on the (1) tactical, (2), operational, or (3) strategic level?

The three levels of military strategy are tactical, operational, and strategic, and the purpose behind a wargame will drive what level the wargame should be designed at.[106] These categories are not hard boxes, and many wargames will incorporate 'leveled' strategies, where there is an overarching purpose and then tactical levels of individual

[103] Curry and Drage, *The Handbook of Cyber Wargames: Wargaming the 21st Century*, 6.
[104] Curry and Drage, 6.
[105] Curry and Drage, 7.
[106] Scott Romaniuk, "Military Strategy and the Three Levels of Warfare" (Defense Report, November 30, 2017), https://doi.org/10.13140/RG.2.2.26287.79528.

battle resolution. However, the levels of military strategy are a useful division for understanding how cyber can be incorporated into wargames and where it fits in depending on the type of game.

The tactical level is considered the most 'micro-level of warfare; it is concerned with single battles or engagements, certain techniques, or individual unit to unit or platoon to platoon conflict.[107] Conflict is short, represented in a few days to a few weeks, and "the combat is not an end in itself; it is the means to achieve goals set on the operational level."[108] The operational level is perhaps the most elusive because it floats between the tactical and strategic levels. However, an excellent example, noted by Luttwak, is the German Blitzkrieg campaign in 1939-1942 – which was an operational strategy, 'lightning war,' where units struck in a rapid, targeted manner creating a series of ideally short and resource-efficient victories. On the tactical level, the unit structure for the invasions seemed "all flank and no 'front'," "very weak" and "highly vulnerable to attacks," but on an operational level, this strategy allowed for a very rapid "tempo and reaction time," which was critical for 'blitzkrieg' warfare.[109] Conflict can be lost or look like a disadvantage for individual squads on the tactical level, but be a win on the operational level.

Colonel Dale C. Eikenmeyer's article in Joint Force Quarterly titled "Waffles or Pancakes? Operational- versus Tactical-Level Wargaming" characterizes the

---

[107] Romaniuk; Edward N. Luttwak, "The Operational Level of War," *International Security* 5, no. 3 (1980): 61–79, https://doi.org/10.2307/2538420.
[108] USAF College of Aerospace Doctrine, Research and Education, "Three Levels of War," in *Air and SPace Power Mentoring Guide*, vol. 1 (Maxwell AFB: Air University Press, 1997).
[109] Luttwak, "The Operational Level of War," 68.

distinguishing factor in the initial question: "Operational wargaming asks, 'Are we doing the right things?' Tactical wargaming asks, "Are we doing things right?'"[110] In other words, the operational level is "what are we doing," and the tactical level is "how we are going to do it."[111] This means that the tactical level is often more technically detailed. An operational planner can begin with more uncertainty and ambiguity, but the tactical level has a pre-designated operational goal to structure around. For the 'board', Eikenmeyer states that an operational level is better laid out on a matrix supported by a map, but tactical, because it is more reliant on geospatial planning and time-distance is better played out on a map with a matrix as support. A tactical game cares about the logistics of resources, time, number of assets, etc. but the operational level uses approximations to determine the sequence of events rather than an exact timeline. In the suggested U.S. doctrine, wargames built for a specific level and purpose look "two levels down": "the operational level looks for the correct assignment of tasks to components one level down and asks whether the component has the correct capabilities two levels down to achieve the assigned tasks…. The tactical level looks at how the subordinate one level down will use assets two levels down to accomplish the task."[112] Different levels of wargaming serve different purposes, for instance, the Joint Operation Planning Process uses operational-level wargaming, while the Military Decision Making Process or Marine Corps Decision Process is tactical.[113]

---

[110] Dale Eikmeier, "Waffles or Pancakes? Operational- versus Tactical-Level Wargaming," *Joint Force Quarterly*, July 2015, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/607625/waffles-or-pancakes-operational-versus-tactical-level-wargaming/.
[111] Eikmeier.
[112] Eikmeier.
[113] Eikmeier.

Lastly, the strategic level looks at the outcome of a conflict, on the whole, the end game or ideal win state. The strategic level incorporates political decision-making as well, to decide what the overall national strategy should be, and how to invest resources to accomplish the steps along the way.[114] A strategic-level wargame could consider the U.S. National Defense Strategy, for instance, and the key would be its overall impact on the international stage, rather than how each aspect broke down into the nitty-gritty of which government agency implemented it in what way.

To put these levels into commercially available games: a tactical game would be "Men Under Fire." With Men Under Fire, players take charge of an individual soldier in a small 6-person unit, and they move through a country-side, represented on a small map, with the group goal of eventually reaching a certain location while clearing structures. The game itself represents a short period, a few hours to a full day, and while the ultimate 'end' of the game is upon traversing the country-side, each soldier has individual goals (such as survive, act as a medic, showcase yourself as brave, remain at the back of each conflict, etc.).[115] On the operational side, there are games like the Battle of the Bulge, which plays out the German Ardennes Offensive in WWII where players control the armies, but still separate them down to individual squadrons and units.[116] And lastly, strategic games like Kriegspiel, The American Civil War, games that play out entire wars and expansive timelines involve "high-level command." [117]

---

[114] Romaniuk, "Military Strategy and the Three Levels of Warfare."
[115] "Men Under Fire," BoardGameGeek, accessed April 5, 2022, https://boardgamegeek.com/boardgame/128490/men-under-fire.
[116] Patrick Carroll, "Strategic, Operational, and Tactical Wargames | Solitary Soundings," *BoardGameGeek* (blog), June 12, 2011, https://boardgamegeek.com/blogpost/2919/strategic-operational-and-tactical-wargames.
[117] Carroll.

However, games can, and often do, incorporate all three levels of warfare into their considerations, particularly the more expansive games. For instance, the game Twilight Imperium, a 3-6 person game of galactic conquest places players as the leaders of space factions attempting to take over the galaxy.[118] The game is played out on large hexes that represent swathes of space, occupied by meteorite belts, planets, supernovas, etc. Players command fleets of ships, but these fleets are split into smaller sections. On the strategic level, there is an overarching war of dominating the empire through military means, on the operational level, this can translate into accomplishing specific objectives, such as defending the center of the galaxy, and a tactical breakdown is showcased in the resolution of individual battles between ships.

A game scenario and purpose will determine at what level conflict should be represented, and then cyber capabilities should be incorporated within the pre-existing conflict. For a 'cyber-in-game' wargame, cyber will slot into an overarching scenario that fits one of the three levels of warfare, but the cyber itself can still be represented across all three levels of warfare. Cyber conflict also can break down into tactical, strategic, and operational levels, which affects the capabilities used in wargame design. This will be addressed further in the capability section.

Is the scenario (1) fictional or (2) realistic?

A game can either be fictional or realistic and be set up in a players versus an environment or players versus each other format. Realistic games require more research for player buy-in, particularly expert player buy-in, and can become out of date as new

[118] "Twilight Imperium: Fourth Edition," BoardGameGeek, accessed April 5, 2022, https://boardgamegeek.com/boardgame/233078/twilight-imperium-fourth-edition.

information is released or conflict situations change. However, realistic games do offer players a greater grounding in realism and increase the ecological validity of the wargame because it is reflective of real-world situations.

Games can be set in a fictional context for multiple reasons:

1. Fictional settings allow for more creativity and flexibility in design.

Fictional settings come with a pre-disposed suspension of belief; players understand that they are not meant to judge the fidelity of the game scenario and instead are forced to trust that the game design fulfills the intended purpose. They also are a clear way to explore the unknown. Sponsored analytical wargames or educational wargames typically want to project into the future, to analyze and prepare for hypothetically upcoming situations, and therefore fictional settings are useful for swapping in and out capability sets, updating entity conflict motivations, and changing the game without having to worry about player buy-in.

2. Fictional teams can help prevent pre-conceived biases on how a certain state should act, or what capabilities a certain state should have.

There are simulations that deliberately abstract from their real-world counterparts to reduce bias and create a more 'blank-slate' motivated combat. One example of this is "We Come in Peace: A game of Explorers and Aliens" which is a free-form role-playing game about mutual resource desire under conditions with a lack of a common language (and therefore stunted communication) to see if agreement can be achieved without conflict.[119] The gameplay is set in a science-fiction scenario, flying aliens in a saucer

[119] Sally Davis, "Review: We Come In Peace, a Game about Cultural Misunderstanding," *PAXsims* (blog), December 12, 2020.

encountering other aliens on an unnamed planet, but at the end of the game, the scenario is revealed to be based upon the Spanish conquistadors' contact with the native population.[120] The reason the game is built to be played 'behind a curtain' is to establish an educational purpose that gets players thinking about the difficulty of cultural misunderstanding and communication and to apply that difficulty to real-world historical examples; a goal that could not be accomplished if players *knew* they were the Spaniards and the native population.

3. Fictional countries can hide preparation intent.

If building a sponsored game, particularly an unclassified one, the United States may not want to project that is wargaming out conflict involving a certain scenario with certain countries. Even with classified games, the possibility of a leak still exists, and because wargaming displays the potential paths in the future, it can also be 'reverse-gamed' by an adversarial country in preparation. While this concern is not at the forefront (a far greater concern is the classification of cyber capabilities), the news that 'the U.S. ran a wargame" versus "the U.S. ran a wargame on battling China for Taiwan" trigger very different levels of attention. The game Hedgemony, RAND's first wargame published for and playable on an unclassified level, is designed for "defense planners, programmers, budgeters, managers, analysts, and policymakers."[121] Players' roles are the United States and key allies and adversaries to set national-level objectives and strategies in a competitive environment. However, an unexpected audience for the game was other countries that took Hedgemony as potentially signaling U.S. strategy, and the game was

[120] Davis.
[121] Michael E. Linick et al., "Hedgemony: A Game of Strategic Choices" (RAND Corporation, September 21, 2020), https://www.rand.org/pubs/tools/TL301.html.

purchased and analyzed outside of the United States.[122] While nothing in the game design would have changed even if designers knew that the game would be analyzed in foreign countries, this still is an example of information sharing that could potentially be detrimental.[123]

4. Fictional countries can also allow pre-modeled frameworks.

The Decisive Action Training Environment (DATE) is a report that lists five fictional, operational environment in the Caucasus region which encompasses real-world Russia and Iran: Ariana, Atropia, Donovia, Gorgas, and Limaria.[124] It provides the strategic setting of each country with various motivations and issues and then gives a list of PMESII-PT variables (Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time) for each country.[125] The DATE reflects some real-world data and events, and through descriptions of their fictionalized situation, real-world connections of the fictional countries can be extrapolated.[126]

Ariana is Iran as "the area's second-largest and strongest nation militarily" with "massive oil and gas reserves in its southwest region along the Persian Gulf." The government wants to spread "its vision of Islamic governance."[127] Atropia is Azerbaijan, a "classic dictatorship" with a "ruling family" that has "significant gas and oil reserves"

---

[122] Wong, Interview with Yuna Wong.
[123] Wong.
[124] U.S. Army, "Decisive Action Training Environment," TRADOC G-2 (Ft. Leavenworth, Kansas: U.S. Army, April 2015), 6.
[125] U.S. Army, 6.
[126] Joseph Trevithick, "The U.S. Army Invented Five Fake Countries," *War Is Boring* (blog), June 16, 2016, https://medium.com/war-is-boring/the-u-s-army-invented-five-fake-countries-58dcc7dad790.
[127] U.S. Army, "Decisive Action Training Environment," 10.

and a large, trans-region petroleum pipeline near its capital.[128] Limaria is Armenia; an "autocracy" with the goal of "survival and advancement of the Limarian ethnicity." [129] Donovia is Russia, "an authoritarian state led by a small, incestuous elite" that wants to place itself in a "co-equal place with the Great Powers of the World."[130] Most countries in the region rely on Donovian military equipment, but there is an ongoing battle between Western hardware and Donovian hardware that has led to Western doctrine slipping into the region.[131] Lastly, Gorgas is "an emerging representative democracy" "in a region driven by group politics and ethnic nationalism" that is reliant on "Western interests" with the smallest military out of the five that want to join NATO.[132]

While, with some guesswork, the countries *closest* to real-world relations can be assumed, the point of these fictional countries is to relate to a variety of real-world countries as contexts and risk measures shift. For instance, a threat tactics report on Syria in 2015 noted that Syria is the most similar to Ariana, but would require additional irregular military forces.[133] The DATE fictional environments are meant to be used and adapted based on the needs of the game, allowing for 'pre-made' flexible frameworks rather than having to design a new model entirely from scratch every time the military wanted to run a simulation.

---

[128] U.S. Army, 10–12.
[129] U.S. Army, 10–12.
[130] U.S. Army, 12.
[131] U.S. Army, 13.
[132] U.S. Army, 13.
[133] U.S. Army, "Threat Tactics Report: Syria" (TRADOC G-2 ACE Threats Integration, February 2016).

Is the conflict in the (1) past, (2) present-day, or (3) speculative future?

Scenarios also affect the time context and the time frame of the game. For instance, most cyber games will be set in the near present or near future, or further future because of the nature of cyberspace and technology – newly developing and utilized concepts. This is also the nature of sponsored games and the military and DOD's desire to be forward-facing. Most commercial and famous games, Axis and Allies and Twilight Struggle, for instance, replay past historical moments like the Cold War or WWII.[134]

Past conflict will be realistic by nature because you are re-gaming history. However, cyber games, even ones set in the current day, are often still fictional in regards to the cyber aspects. This will be addressed further in the cyber capability section. The distinction between 'present day' and 'future' is blurred because most wargames set in the present day represent hypothetical scenarios, but conceivable ones – such as a potential future conflict over the South China Sea, over Taiwan, a nuclear war, etc. For example, the Pentagon ran a wargame during the Afghanistan conflict to evaluate two military options: a counter-insurgency campaign with 44,000 troops or an additional 10-15,000 more soldiers to a "counterterrorism plus" effort.[135] The goal was to evaluate how stakeholders like the Taliban, NATO, and involved governments would react to either option. Even though this game, at that time, would be set in the 'near future' it refers to a present-day conflict. Therefore, the 'future' distinction in this refers to the speculation of

---

[134] "Axis & Allies | Board Game | BoardGameGeek," BoardGame Geek, accessed April 4, 2022, https://boardgamegeek.com/boardgame/98/axis-allies; "Twilight Struggle | Board Game | BoardGameGeek," BoardGame Geek, accessed April 4, 2022, https://boardgamegeek.com/boardgame/12333/twilight-struggle.
[135] Greg Jaffe and Karen DeYoung, "U.S. Tested 2 Afghan Scenarios in War Game," October 26, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/25/AR2009102502633.html.

a wargame past the extent of current knowledge or the 'speculative' definition that McGrady gives.

Speculation

An important aspect when it comes to cyber wargames specifically is the level of speculation, which can affect all levels of content and structure format. Because cyber wargames deal specifically with cyberspace or technology that is unpredictable because of a lack of information – whether that lack of information is derived from classification levels, the lack of observed empirical evidence, or because the addressed technology has not been invented or tested – there is no 'right' way to run or adjudicate the game. The game designers have no way of knowing what would happen in the future, and, more importantly, *neither does anyone else.*

Speculative games pose a unique challenge alongside adjudication and realism, which is the issue of 'fighting the system." McGrady defines speculative games with three conditions, representing: a future that is not a simple extrapolation of the current day, a narrative that does not fit easily with players' worldview and goes beyond current understanding.[136] McGrady refers to this as a violation of the "dramaturgical expectations," and he gives the example of a wizard showing up in the game, or a typhoon blowing out an operation.[137] Both cause a player dissonance with the expectations of the real-world and therefore real-world applicability or they cause dissonance with what the player is willing to stretch within the fictional world of the game. (Typhoons are not unheard of, but it feels 'unfair' for a random one to sweep into a

[136] Ed McGrady, "Building Speculative Games," Representing Artificial Intelligence in Wargames (Connections 2020, December 2020), 12.
[137] McGrady, 7.

game that is not about typhoon control, and wizards do not exist.) However, it is for this exact reason that cyber wargames are important because they are flexible enough to deal with the undefined, whereas other analytical or predictive methods may be too stringent for the mental creativity that hypothetical cyber operations require.[138] After WWII, Admiral Nimitz noted that: "The war with Japan had been reenacted in the game rooms at the Naval War College by so many people and in so many different ways, that nothing that happened during the war was a surprise . . . absolutely nothing except the kamikaze tactics toward the end of the war; we had not visualized these."[139] Speculative games that explore possibilities that are outside the realm of current-day plausibility can help capture future concepts of warfare and technology.

Is the conflict (1) versus an environment or (2) versus other players?

The scenario will determine whether or not the game is adversarial or cooperative for players. If the players are playing together against an environment (or a game master) then it is cooperative. If the main focus of the game pits players against each other, then it is adversarial.

Cyber Elements:

There are a variety of ways to represent cyberspace operations and conflict within a wargame. However, there are several design choices that a game must choose between.

---

[138] McGrady, 9.
[139] David Banks, "War Games Shed Light on Real-World Strategies," The Conversation, April 19, 2019, http://theconversation.com/war-games-shed-light-on-real-world-strategies-113631.

Focus of the Operation or a Support of the Operation

Cyber conflict does not exist within a vacuum. As noted, cyber conflict can exist in the gray zone between peace and war, and therefore cyber wargame representation of cyber is also varied depending on the scenario. Cyber capabilities can be designed to reflect a pure cyber conflict, or they can be designed as a supporting factor for a larger scale operation. McGrady's games, for example, "treat cyber as a force multiplier or an erosional effect that throws sand in the gears of operational efficiency."[140]

If a cyber capability is integrated into a larger operation, then an important aspect of game design and adjudication is ensuring that the cyberspace conflict connects with other functions, otherwise, cyber becomes one-off events that are interesting and important on a grand scale, such as knocking out a power grid, but do not impact players in the granular sense.[141] Vogt gives the example of attacking a port versus a distributed network:

> "If you cyber-attack a port, it's easy. You can't visit the port, ships can't leave, there's no fuel. It's harder when it's a distributed network where the second and third-order effects are less known. For instance, if you're in the Department of Defense, you book through the Defense Travel System. It's how you get your car, your hotel, etc. If that went down, it would cause utter chaos across the entire globe, but, this is a micro-scale that only impacts tens of thousands of people. Figuring out how to represent this impact in a game is much harder"[142]

---

[140] McGrady, "Building Speculative Games," 24.
[141] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[142] Marrin, Vogt, and Pellegrino.

If cyber operations exist on their own, it is a cyber wargame, if they are launched in support of or attached to broader goals, then it is a cyber-in-game.

Fixed or Matrix'd

Cyber capabilities can be 'fixed' or they can be 'matrix-style.' In the first option, they are 'given' in a set list, often a card deck, by the game designer, in the second, they are created by the player imagination. This operates on a sliding scale, for instance, the designer could give a very strict set of capabilities with designated interactions and point values, and players are only allowed to use those cards, or a player can describe how they would use the given capabilities for an intended effect and be awarded based on adjudication for the soundness of their argument, or a player could just be given the requirement of attack and defend and be required to explain how they plan on accomplishing that general goal.

Argumentation Mechanics

Matrix games can rely on 'argumentation mechanics' which reward players based on how creative and convincing their argument is to the adjudicator, or to their fellow players – whichever entity operates as the 'control cell.' For cyber wargames, this will be built into the game as the players try to convince the adjudicator that they have successfully hacked and launched their cyberspace operation because of their prep work or a lack of defenses from the other side, and therefore should receive a certain effect. Or, players will try to convince each other or the other team to change the probability roll for a higher chance of success.

Tactical, Operational, and Strategic

Cyber capabilities can also correlate to the tactical, operational, and strategic levels, although literature attempting to distinguish between these levels is sparse. Strategic cyber attacks are described as very large-scale, sometimes damaging attacks for strategic objectives. Some authors have described strategic attacks as 'stand-alone' operations that do not support or require other conventional domains of warfare.[143] It is unclear whether or not any examples of strategic cyber operations have occurred in real-life. Stuxnet is the closest possibility, however, Stuxnet's objective does not necessarily fit into a strategic level of warfare, given its limited intended purpose.[144] Even during the current Russia-Ukraine conflict, there has been a surprising lack of catastrophic, strategic level cyber operations.[145]

Operational level cyber capabilities focus on advantages in campaigns and battles. Gartzke and Sanger characterize operational attacks as happening in conjunction with other military forces as a supporter.[146] Lastly, tactical attacks, if they were to correlate to

---

[143] Martin C. Libicki, "Crisis and Escalation in Cyberspace," January 3, 2013, https://www.rand.org/pubs/monographs/MG1215.html; Jon Arquilla, "The Rise of Strategic Cyberwar?," *Communications of the ACM* (blog), September 25, 2017, https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext; G. Visky, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations," 2020, https://www.semanticscholar.org/paper/Cyber-in-War%3A-Assessing-the-Strategic%2C-Tactical%2C-of-Visky/fdf5e3f147b8447f699d5b60c8da4e3c78b94e4a.

[144] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishing Group, 2014).

[145] Kari Paul, "'Catastrophic' Cyberwar between Ukraine and Russia Hasn't Happened (yet), Experts Say," *The Guardian*, March 9, 2022, sec. Technology, https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.

[146] David Sanger, "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age" (Wilson Center, 2018); Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73.

the traditional levels of war, should focus on smaller battles. Metcalf and Barber describe this as "at battalion level or lower."[147] In practical terms, the development of tactical cyber has been hindered because most cyber operations are coming out of U.S. Cyber Command, rather than individual hackers stationed with a unit. Tactical cyber should be "something that does not require a lot of intelligence, does not require a great deal of sophistication and stealth, delivers effects that can be completely contained within a specific battlespace, and can be monitored, reported, and measured accurately and efficiently."[148] However, Visky proposes that because "the tactical level thus deal with the conduct and movement of troops in a given terrain," operations that affect this, even if they are not necessarily targeting an individual unit, can be classified as tactical cyber – for example, a cyber operation that takes over the cameras in an area to provide situation awareness or a GPS operation. [149]Deciding what level to portray cyber on will affect the capability set of the game. In general, the higher the technical level of detail, the lower the level of warfare.

Covert or Overt Mechanism

Cyber capabilities are typically covert because of the strategic advantage that secrecy provides, however, this makes running a game more complicated because adjudication must then happen on multiple levels. While covert mechanics are more realistic, they also make the game itself harder for players because it adds a dimension of imperfect knowledge. As with other design decisions, the covert-overt mechanism, also

[147] Andrew Metcalf and Christopher Barber, "Tactical Cyber: How to Move Forward," *Small Wars Journal*, September 14, 2014, https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward.
[148] Metcalf and Barber.
[149] Visky, "Cyber in War," 186.

known as the information problem, can exist on a spectrum. Designers can provide players with complete and perfect information, where all moves happen in a turn-cycle, all moves are publicly announced, and all effects are announced before the next team takes the turn. At the other end of the spectrum is where all moves are covert, and adjudication happens at certain points within the game to announce the effect or discovery of covert actions when it relates to win conditions. Smaller-scale games will typically lean more towards overt information, while larger-scale games will have imperfect information elements due to scale and greater adjudication bandwidth.

Past, Present, and Future

This paper is not particularly concerned with the cyber capabilities of the past because it does not see a high educational or analytical value derived from looking back at previous conceptions of cyberspace. However, the present and the future capabilities are particularly relevant to creating parameters for the cyberspace of the game, as well as affect realism and believability. Similar to the scenario setting in the present and the future, this distinction is blurry because of secrecy.[150] Cyber exercise designers creating unclassified capability sets based on open-source material could be using past technologies that are outdated, or, if they are speculating, they could be hitting on accurate, current cyber capabilities or capabilities in development.

[150] I visited the International Spy Museum in D.C. last summer, and I found some of the technology that was declassified fascinating and outside the scope of my imagination. However, the only reason, assumedly, that the spy technology was declassified is because the U.S. already has technology that far outpaces it. The same is true for cyber capabilities, where what seems cutting edge in the public eye may already be rendered obsolete compared to classified technologies.

McGrady suggests three methods for engineering future technology: extrapolation – starting from what technology is known and then extrapolating what it would look like X years from now, interpolation – creating a starting point and an end point and then seeing what would happen between the two, and Imagineering – trying to create imaginary engineering on new technologies to see how they could function.[151] He gives the example of trying to define a seventh-generation fighter. Extrapolation suggests that the seventh-generation fighter would have longer-range weapons, sensors, and more advanced mission control. Interpolation would try to picture the ranges that the seventh generation could take – small and drone-like or giant aircraft-esque and its building on the sixth generation. Imagineering would give the seventh generation the ability to manipulate the electromagnetic spectrum and control waveforms registered from the aircraft. Noting what 'timeline' cyber capabilities exist in is important because it also lends to the fidelity and realism of the game; are these cyber capabilities confirmed to be in existence, or are they educated guesses?

Fidelity and Realism

The fidelity of a game refers to how realistic it is: in a broad sense, how well the game and the interactions within the game imitate the real-life environment. High fidelity does not automatically make a game more successful. Games are an abstraction of reality for a reason because many aspects of the real world can or must be ignored to produce a useful game. For video games, high fidelity often refers to two aspects: graphical effects and physics effects. A game that is highly technically accurate, with photo-realistic

[151] McGrady, "Building Speculative Games," 17.

graphics and an interactive environment – rain that hits armor or humidity that affects shooting conditions, is praised for its high fidelity. However, for wargames, fidelity is judged differently.

For instance, the Air Force Materiel Command (AFMC) has five principles for high fidelity games;

"1. Concept descriptions have to be accurate

2. blue players must employ concepts and systems accurately

3. adjudication must be correct

4. red players have to counter blue players appropriately

5. people with experience in analysis have to assess the game."[152]

For cyber space interactions in wargames, fidelity becomes a difficult issue because, unlike combat simulations where models can be built of pre-existing data of how fast a bullet or tank can travel under certain conditions, there is no one 'correct' model for cyber space. A hack that could work one day could completely fail the next without anything changing from the 'blue team' in real life. Add to that the 'fog of war' which essentially covers all of cyberspace, and judging fidelity is incredibly difficult, even for cyber experts.[153] So fidelity can be broken down into two parts, the cyber content/capabilities and the resolution of their effects, which means adjudication is crucial. The fidelity of the game impacts the ecological validity of the game, the "extent to which behavior under test conditions mirrors real-world behavior," and wargames with a high ecological validity allow analysts to "use wargames to realistically simulate and

[152] Wong et al., "Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action," 99.
[153] Interview with Unnamed Source.

study foreign policy decision-making processes."[154] Lin-Greenberg, Pauly, and Schneider find "ecological validity to be a key element of external validity – the generalizability of research findings beyond the research context."[155] While external validity is more relevant for analytical games, it is also important for education games because players need to be able to generalize their in-game knowledge for out-of-game, real-world scenarios.

The fidelity/realism of a game specific to its cyber aspects can be broken down into what, how, and why. What techniques or tools are used, how are they used (how is the system hacked through what intrusion methods), and why was the operation launched (what were its intended effects)? All three aspects bring with them their own level of technical detail, and designing a cyber wargame requires a balance of what level of detail is useful for the game and the intended participants versus over-complicating or oversimplifying the methodology, speculating too much, or getting into classification concerns.

What, How, and Why

The what represents what cyber techniques or tools are used? The how and the what often overlap, but they can have distinctive features. For instance, you design a worm, which is the what, but that virus is delivered via a casually dropped USB in a parking lot or via a spam email, which is the how.

[154] Lin-Greenberg, Pauly, and Schneider, "Wargaming for International Relations Research."
[155] Schechter, Schneider, and Shaffer, "Wargaming as a Methodology."

The why is the effects. Abstraction into an effects-based model for various game mechanics is common: we do not care how something happens, only what it does at the end – the why of the cyber operations. For example, a player launches a non-descript virus, and a ship's targeting capability is jammed. For this particular game, the player does not need to know what virus was developed, what the operating system the ship's targeting capability ran on, how the virus was connected to the system, what firewalls it needed to bypass, how the targeting system was disabled by the virus – they just need to be aware that they can no longer utilize their ship's targeting system and whether this is a permanent or temporary effect.

Effects-based is the default that most unclassified cyber games use because it has the lowest knowledge and classification barrier, the least need for speculation regarding specificity, and the least technical knowledge required. In general, classified games will also be centered around effects-based cyber as well if they are made for non-technical decision-makers.[156]

The Cyber Kill-Chain

Who launches what against whom, why, and how?

If you were to build the perfectly realistic highest-fidelity cyber wargame, what would this include? One way to go about this is to look at the technical attack chain.[157] A cyber

[156] Lea, Interview with Kate Lea.

[157] One of the best ways I have seen this done was in the Dtsl's Cyber Card Game, developed in the United Kingdom, found in Chapter 4. Tom Mouat, "Cyber Card Game" (Wargame Session, Georgetown Wargaming Society, Dtsl UK, February 13, 2022).

attack lifecycle, also known as the 'kill chain' has been conceptualized in different manners. For instance, Lockheed Martin and MITRE give a seven-step process:[158]

1. Reconnaissance
2. Weaponization
3. Deliverance
4. Exploitation
5. Control
6. Execution
7. Maintenance

Mandiant Consulting, part of FireEye – a cybersecurity company, conceptualizes a similar phase model and provides examples of techniques, broadly, as well as specific technical techniques:[159]

1. Initial Recon
2. Initial Compromise
3. Establish Foothold – Maintaining control through methods like installing a backdoor
4. Escalate Privilege – Gaining further access, i.e. via keystroke logging, authentication subversion, etc.
5. Internal Recon

[158] MITRE, "Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle" (The MITRE Corporation, 2015), http://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf.
[159] Mandiant, "Targeted Attack Lifecycle | Mandiant," 2022, https://www.mandiant.com/resources/targeted-attack-lifecycle.

6. Move Laterally – Moving to additional systems, often via escalating privilege, such as remote commands and logins or network share files
7. Maintain Presence
8. Complete Mission

Within the kill chain lifecycle, there are also technical techniques; The MITRE ATT&CK Matrix offers an expansive overview of attack techniques, the 'how' or 'what,' organized into tactics, the 'why.'[160]With 14 tactics: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defensive Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact, each with 7 to 40 techniques for a total of over 200 techniques, and some techniques having multiple subtechniques, the methods for a cyber-attack are countless, even without getting technically specific. The techniques include general methods like acquiring infrastructure (technique) through domains, DNS Server, Virtual Private Server, Server, Botnet, and Web Services (subtechniques).

There is also a defender-counterpart to the attack lifecycle, although this is less defined in the industry. MITRE sorts the goals for a response into six different purposes:[161]

"Divert the adversary's efforts" through *deterrence* or *misdirection*

"Preclude the adversary's specific efforts from having an effect" through *negation or preemption*

[160] MITRE, "MITRE ATT&CK®," 2021, https://attack.mitre.org/.
[161] For the full MITRE attack matrix, please see the appendix. MITRE, "Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle."

"Impede the adversary," forcing a greater resource or action investment through *degradation or delay*

"Detect the adversary's activities" or "Limit the adversary's effectiveness" through *containment, curtailment, recovery, or expungement*

"Expose the adversary" through *analysis* or *publicity* [162]

Given the extensive length of a cyber attack lifecycle, without even considering specific technical cyber tools, a wargame needs to cut down the representation of this lifecycle to what is needed. A real-world representation of this kill chain would be live hacking, but this is not useful to decision-makers, nor is it a wargame.

This is where designers must balance between *fidelity* and *utility*. There must be enough detail included so that participants feel like they are conducting realistic attacks, but not too much detail that the game becomes bogged down or it is not relevant to the win condition. There is no perfect answer for judging the level of technical detail, it is up to the game and the participants. Fidelity and realism are not important just for deriving results that could be useful for real-world application, it is also crucial for participant buy-in. Abstract or speculate too heavily, and players will no longer buy in to the game. McGrady notes that "you have to create acceptance amongst the players that whatever you are doing with the technology is fair and accurate."[163] However, it also needs to be at a level of understandability for the players. Abstraction is necessary to facilitate communication between different players. If the game is intended for cyber experts talking to cyber experts, then that will be more technical, decrease abstraction and

[162] For the full MITRE attack matrix, please see the appendix. MITRE.
[163] McGrady, "Building Speculative Games," 16.

increase fidelity. However, if a game places technical and non-technical people together in a room, not a lot will get done unless there is a translation mechanism between the two – which can be an abstraction or a decrease in technical realism.[164] While the first aspect of fidelity is on the actual capability sets, the second is the resolution of using those capabilities, which is dependent on adjudication.

Adjudication

Based on a MORS Professional Gaming Workshop and the McHugh's glossary of wargaming terms, there are four types of adjudication:[165]

Free: Based on expert opinion of adjudicators alone.

Rigid: Based on pre-established rules and models.

Semi-free: Rigid that can be adjusted or changed by adjudicator opinion.

Consensus: Collective decision-making, often including opposition and adjudicators.

Argumentation mechanics can play into free adjudication, semi-free, or consensus.

Adjudication is done by the control cell or the facilitators of the game. Adjudication is very tricky: it can set the entire tone of the game, shift the tides of victory, or guide a game to a certain end. For instance, the allegory of "We Come in Peace" can only be communicated by Control. Sally Davis, senior analyst at the UK's Defense Science and Technology Laboratory, ran a session as Control and wrote up her experiences, explaining that: "it's Control's job to take everything the players say, translate it into the hidden scenario to determine the outcome, and then back into the sci-

[164] Sepinsky, Interview with Jeremy Sepinsky.
[165] Francis McHugh, "Appendix C - A Glossary of War Gaming Terms," in *Fundamentals of War Gaming*, 3rd ed., 1966; William L. Simpson Jr., "A Compendium of Wargaming Terms" (MORS, September 20, 2017), www.mors.org/communities/wargaming.

fi allegory to communicate the effect to the players."[166] In this particular session, the outcome was relatively peaceful with no threats of war, because the stakes of the game, to the players, were "we'll make friends? When it should have been you face death and/or cultural extinction."[167]

Marrin, Vogt, and Pellegrino advocate for an 'invisible' method of adjudication, where players believe that any consequences of their actions are not a function of adjudication, it is an outcome of the other team.[168] Adjudication must happen quickly because it gives players the information needed for their next step. However, Marrin, Vogt, and Pellegrino place less value on adjudication as having a 'right' or 'wrong' answer to player action, instead, adjudication "provides a plausible outcome back to decision-makers to let them make another decision." [169] They utilize a 'goal-post' analogy, where an action can have a range of outcomes (our best day on an adversary's worst day and vice versa). As long as the outcome falls within the 'goal posts of plausibility,' then the adjudication is valid.

Simulating the 'Fog of War': Uncertainty and Unpredictability in Adjudication

Adjudication and game design play a role in the fidelity of cyber wargames. The more a cyber wargame can imitate the constantly shifting, creative methods of cyber conflict, the more realistic it will appear to players. One way of achieving this is through the matrix or free form capabilities, divergent paths of success, and chance-based success

[166] Davis, "Review: We Come In Peace, a Game about Cultural Misunderstanding."
[167] Davis.
[168] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[169] Marrin, Vogt, and Pellegrino.

rolls with modifiers. Matrix and free form capabilities allow players to apply their technical expertise and creativity to cyber attacks, simulating the uncertainty and unpredictability of cyber warfare. This also avoids creating fixed 'action-reaction' capability paths, where a certain card capability explicitly counters another. However, this is reliant on players having the background knowledge necessary to create a highly realistic game. In some cases, particularly for games built for non-cyber-experts, fixed card sets can be more helpful because it shows the possible applications of cyber warfare created by cyber experts. Divergent paths of success allow for more player creativity, rather than linear methods to success; this returns to Curry and Drage's description of train-stop games versus choose-your-own-adventure or interactive cyber games.

Chance and dice rolls are a common mechanic in wargaming, particularly for cyber wargames, because it represents a success-burn ratio. This applies to the goalpost analogy that Marrin, Vogt, and Pellegrino refer to; dice rolls help simulate the chance of a 'good day' and 'bad day' with cyber capabilities or can help account for a lack of knowledge regarding cyber capabilities. There is no good answer for what a proper success-burn ratio is because all cyber operations resolutions are ultimately a best guess; some games use a close to 50-50 ratio, others use an 80-20 ratio, there is no constant, nor is there any solid evidence behind a ratio of success.[170] However, using a pre-determined ratio that can be modified helps with player strategy because they can plan around probabilities of success and failure and are encouraged to think creatively to improve their chances.

[170] Lea, Interview with Kate Lea; Bae, Interview with Sebastian Bae; Haggman, Interview with Andrew Haggman.

Data Generated, Collection Methods, and Data Analysis

Wargaming generally generates two types of data: outcome data and deliberation data.[171] The former encompasses the results of the game, while the latter is focused on how participants reached those results. Deliberative data can showcase decision-making processes, while outcome data can demonstrate one potential outcome of a certain scenario during a single run of the game. As has been emphasized multiple times throughout the thesis, it is important that outcome data is not taken as what will happen in an actual scenario.

There are different levels of data capture, depending on the tools that are used. Imagine at the highest point on the spectrum is an all-encompassing surveillance machine that records all conversations and interactions between players as well as adjudication and discussion in the backroom. This is, while not impossible, a massive investment of resources with a limited pay-off due to introducing a new problem of data overload. Additionally, while all players are aware that wargames are being observed and analyzed to some degree, more obvious methods of higher degrees of observation can worsen the "Hawthorne effect," where players modify their behavior to the point of impacting game results.[172] Wargames that are run digitally can also collect more data than their in-person counterparts at a lower cost. The SIGNAL (Strategic Interaction Game Between Nuclear Armed Lands) game has an in-person board game version and an online version; the online version has an "automated collection of player decisions, demographic data, and

[171] Lin-Greenberg, Pauly, and Schneider, "Wargaming for International Relations Research."
[172] G. Wickström and T. Bendix, "The 'Hawthorne Effect'--What Did the Original Hawthorne Studies Actually Show?," *Scandinavian Journal of Work, Environment & Health* 26, no. 4 (August 2000): 363–67.

chat feeds used in diplomacy… scalable data collection."[173] The amount of data a wargame requires will ultimately circle back to its purpose. An analytical game will, in general, require more data than an educational game, in regards to deliberation and outcome.

SIGNAL also uses survey data where players "are asked a series of questions that closely approximate the strategic decisions faced by players within the board and electronic variants of the SIGNAL wargame."[174] Surveys are commonly employed by designers to capture more deliberative data, and to understand the thought process behind an action from an individual perspective. They can also be used to capture team dynamics that may skew outcome results, by allowing players to express their personal decision-making preferences and perception of ability to enact those preferences within a game.

Wargames typically produce qualitative data, and so analysis of the data is up to the analysts on the team. Wargames very rarely publish the data captured, and therefore the conclusions of a wargame are often taken at face value. Criticisms of the game results will typically be directed at game design and fidelity or participant selection rather than data analysis. For analytical games and educational games alike, the importance is the information derived from the game, either from new information for players or new information for sponsors. Dr. Yuna Wong, designer at IDA and adjunct professor at Georgetown, calls this the "Schelling" test, also referenced in David Banks, co-founder of the Wargaming Network at King's College London article on how "War games shed

---

[173] Bethany Goldblum, Andrew Reddie, and Jason Reinhardt, "Wargames as Experiments: The Project on Nuclear Gaming's SIGNAL Framework," *Bulletin of the Atomic Scientists* (blog), May 29, 2019, https://thebulletin.org/2019/05/wargames-as-experiments-the-project-on-nuclear-gamings-signal-framework/.
[174] Goldblum, Reddie, and Reinhardt.

light on real-world strategies": "one thing a person cannot do, no matter how rigorous his analysis or heroic his imagination, is to draw up a list of things that would never occur to him."[175] The "Schelling Test" asks for any new insights derived from the gameplay itself and the interactions of the participants. The most important thing for wargame data generation and analysis is to produce useful information that is in line with its original purpose.

[175] Banks, "War Games Shed Light on Real-World Strategies."

Chapter 3. Analyzing Cyber Wargames

This section will analyze cyber wargames in three sections, modifying the Connections Conference's purposes of "decision-making, education and training, and recreation" as analytical, educational, and entertainment/recreational/educational."[176] For a breakdown of elements of the games, please refer to the summary table below.

Cyber Wargame Summary Table

Game	Purpose	Specific Objective	Sponsor	Format	Participants	Participant Interactions: Cooperative Non-Cooperative	Adjudication: Free Rigid Semi-Free Consensus	Cyber Representation: Cyber Game or Cyber-In-Game Fixed or Matrix'd Tactical, Operational, or Strategic Covert or Overt Past, Present, or Future Capabilities Technical Detail Level Cyber Kill Chain: Cause or Effect Chance Mechanics	Data Generated	Ideal Outcome	Audience of Outcome
Cyber Storm Series	Test the Effectiveness of Current or Future Cyber Response Policies	See Cyber Storm Comparison Table	DHS National Cyber Security Division	Single-sided, seminar-style game	Public and Private Sector	Cooperative	Free	Cyber Game Fixed or Matrix'd: N/A Strategic Overt Present Capabilities Technical Detail: Low Cyber Kill Chain: Effects-Focused Chance Mechanics: N/A	Player Deliberation	Understanding of the current state of communications and recovery during a cyber attack and improvements going forward	Players and the organizations and agencies they represent
Global Title X 10	Innovation (Non-Cyber)	Find the catalyst for instability, impediments, and solutions for maritime	U.S. Navy	Single-sided, seminar-style analytical game	Defense and Military Experts	Cooperative	N/A	N/A	Player Deliberation	Participant Learning Generation of Recommendations	Unclassified Report generated

[176] "Wargaming."

		regional and cross-regional partnerships									Shared with Navy Sponsor
Global Title X 13	Test Potential Future Structures	Analyze which C2 system out of three is best to command and control combined forces for cross-domain operations in a high-intensity A2/AD environment	U.S. Navy	Single-sided, seminar-style analytical game	Defense and Military Experts	Cooperative	Free	Cyber-In-Game Fixed or Matrix'd: N/A Operational Overt/Covert: N/A Present Capabilities Technical Detail: Medium Cyber Kill Chain: Effects-Focused Chance Mechanics: N/A	Player Deliberation and Outcome	Utilize hypothetical C2 systems analysis for integrating into the current C2 structure	Unclassified Report Shared with Navy Sponsor
Global Title X 14	Test Potential Future Structures	Identify strengths and weaknesses of the four C2 attributes and improvements to the draft CONOPS	U.S. Navy	1.5- sided, seminar-style, analytical game	Defense and Military Experts	Cooperative (Adversary played by Naval War College)	Free	Cyber-In-Game Fixed or Matrix'd: Fixed Operational Overt Present Capabilities Technical Detail: Medium Cyber Kill Chain: Disablement Point and Causal Chance Mechanics: N/A	Player Deliberation and Outcome	Create recommendations for the C2 systems going forward	Unclassified Report S shared with Navy Sponsor
Defend Forward	Test the Effectiveness of Current or Future Cyber Response Policies	Exercise the "Defend Forward" doctrine	DOD	Two-sided, seminar-style analytical game	Public-Private Sector	Adversarial	Free	Cyber-In-Game Fixed or Matrix'd: Fixed Options, Matrix Execution Strategic Overt and Covert Present Capabilities Technical Detail: Medium Cyber Kill Chain: Access and Causal Chance Mechanics: N/A	Outcome Results	Analyze the outcome of a Blue State enacting "Defend Forward"	Unclassified Report Findings shared with Department of Defense
Merlin	Act as a Communication Tool Between Cyber and Non-Cyber Experts	Spark creative thinking about cyber tradecraft and resource trade-off	Air Force	One-sided, seminar-style module	Cyber and Terrestrial Operators	Cooperative	Free	Cyber-In-Game Fixed or Matrix'd: Fixed Options, Matrix Execution Tactical Overt and Covert Present Capabilities	N/A	N/A	N/A

								Technical Detail: Dependent on Player Creativity Cyber Kill Chain: Target, Access, and Causal Chance Mechanics: 80-20 Baseline Burn			
Hybrid Threat Rising	Education of Non-Experts	Exploration of Multi-Domain Conflict	Women in Command	Two-sided, tabletop game	Women from 18-to 30 who don't know a lot about defense or military operations (Other Played): Government officials, Military training, etc.	Non-cooperative	Rules	Cyber-In-Game Fixed or Matrix'd: Fixed Operational Overt Present Capabilities Technical Detail: Low Cyber Kill Chain: Causal Chance Mechanics: Success-Burn Ratio	N/A	N/A	N/A
Cyber Card Game	Identify Potential Failures or Weak Points	Thinking like an Attacker to target a port	UK's Dstl	One-sided, seminar-style game	UK Officers	Cooperative	Rules	Cyber Game Fixed or Matrix'd: Fixed Tactical Covert with Discovery Mechanics Present Capabilities Technical Detail: High Cyber Kill Chain: Start to Finish Chance Mechanics: Success-Burn Ratio	N/A	N/A	N/A
Littoral Commander	Speculate on Future Technology Capabilities and Scenarios	Future Warfare Simulation	Personal Project	Two-sided, hex boardgame	Officers	Adversarial	Rules	Cyber-In-Game Fixed or Matrix'd: Fixed Tactical Covert Capabilities, Overt Execution Future Capabilities Technical Detail: Medium Cyber Kill Chain: Effects-Based Chance Mechanics:	N/A	N/A	N/A

								Success-Burn Ratio			
Cyber Security Strategy Game	Exercise a Cyber Response Plan with a Cyber Attack Scenario	Government Cyber Security Education	Academia Project	Table-top, dual-sided, rule-based game	All – academia, civilian, military, government (more specifics can be found in Appendix C: Game Sessions (297). Intended for non-specialists.	Non-Cooperative	Rules	Cyber Game Fixed or Matrix'd: Fixed Operational/Strategic Overt Present Capabilities Technical Detail: Low Cyber Kill Chain: Effects-Based Chance Mechanics: Success-Burn Ratio	N/A	N/A	N/A
Enterprise Defender: Protecting a Modern Business	Education of non-experts And Testing of Current Plans	Education of non-IT managers to understand risks and develop action plan	Personal Project	Dual-sided, one-phase game	Intended for non-IT experts	Adversarial	Free	Cyber Game Fixed or Matrix'd: Matrix Tactical Covert Present Capabilities Technical Detail: Dependent on Player Creativity Cyber Kill Chain: Dependent on Player Creativity Chance Mechanics: N/A	N/A	N/A	N/A
Hacker	Teach Non-Experts Cyber Concepts	Entertainment	Profit	Multi-sided Card-Board Game	Public	Adversarial	Rules	Cyber Game Fixed or Matrix'd: Fixed Tactical Overt Present Capabilities Technical Detail: High Cyber Kill Chain: Intrusion and Access Chance Mechanics: Success-Burn Ratio	N/A	N/A	
[dx03d!]	Teach Non-Experts Cyber Concepts	Entertainment	Profit	One-Sided, Card-Board Game	Public	Cooperative	Rules	Cyber Game Fixed or Matrix'd: Fixed Tactical Overt	N/A	N/A	N/A

								Present Capabilities Technical Detail: High Cyber Kill Chain: Intrusion and Access Chance Mechanics: Card Draw			
Collection Deck	Teach Non-Experts Cyber Concepts	Education of Intelligence Collection Techniques and Disruptive Obstacles	CIA	Two-sided Card Game	CIA Agents	Non-Cooperative Other Players Play as Environment	Free Consensus	Cyber-In-Game Fixed or Matrix'd: Fixed Tactical Overt Present Capabilities Technical Detail: Low Cyber Kill Chain: Effects-Based Chance Mechanics: N/A	N/A	N/A	N/A
Collect It All	Teach Non-Experts Cyber Concepts	Entertainment	Profit	Two-sided Card Game	Public	Non-Cooperative Other Players Play as Environment	Free Consensus	Cyber-In-Game Fixed or Matrix'd: Fixed Tactical Overt Present Capabilities Technical Detail: Low Cyber Kill Chain: Effects-Based Chance Mechanics: N/A	N /A	N/A	N/A
Influence 2040	Speculate on Future Technology Capabilities and Scenarios	Education on Future Intelligence Warfare Techniques	ODNI	Two-sided Card Seminar Game	ODNI Agents	Adversarial	Free	Cyber-In-Game Fixed or Matrix'd: Fixed Operational Overt and Covert Future Capabilities Technical Detail: Low Cyber Kill Chain: Effects-Based Chance Mechanics: N/A	N/A	N/A	N/A

Analytical

Analytical wargames are intended to derive information, and most commonly create lessons learned or findings and recommendations. While these lessons do not have to be actionable, the ideal goal is that if they are not immediately actionable, they can spur future research and decision-making. Therefore, this section will look at what the goal of the game was, how the representation of cyber and conflict contributed to that goal, and whether or not it was achieved.

Cyber Storm Series

Cyber Storm is a cyber wargame series, the 2022 version being the eighth and most current version, recently run in March 2022. The series began in 2006 and is run about every two years, with subsequent versions in 2008, 2010, 2011-2014, 2016, 2018, 2020, and 2022.[177] Each game is accompanied by a final, declassified report, except for the latest 2022 version. For abbreviated, quoted, direct comparison of the goals and objectives, and findings of each Cyber Storm iteration, see the available table in the Comparison Section.

Cyber Storm I

The 2006 game was sponsored by the Department of Homeland Security's National Cyber Security Division, a division that, at that time, was responsible for cyber security coordination and considered "a focal point for the Federal Government's interaction with state and local government, the private sector, and the international

[177] CISA, "Cyber Storm: Securing Cyber Space | CISA," accessed April 14, 2022, https://www.cisa.gov/cyber-storm-securing-cyber-space.

community concerning cyberspace vulnerability reduction efforts."[178] Cyber Storm 2006 was considered the first "government-led, full-scale cyber security of its kind" that brought together over 100 different participants from the public and private sectors.[179] The goals of Cyber Storm I were to "stimulate participants to:

- Exercise interagency coordination (e.g., standard operating procedures, communications, and decision support mechanisms) through the activation of the NCRCG [National Cyber Response Coordination Group] and the IIMG [Interagency Incident Management Group]
- Exercise inter-governmental (international) and intra-governmental (Federal-State) coordination and incident response
- Identify policies/issues that hinder or support cyber security requirements
- Identify public/private interface communications and thresholds of coordination to improve cyber incident response and recovery, as well as identify critical information sharing paths and mechanisms
- Identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public
- Identify cyber physical interdependence of infrastructure of real-world economic and political impact"[180]

Secondary Goals:

---

[178] National Cyber Security Division, "Cyber Storm Exercise Report" (Department of Homeland Security, September 12, 2006), 3, https://www.cisa.gov/cyber-storm-i.
[179] National Cyber Security Division, "Cyber Storm Exercise Report."
[180] National Cyber Security Division.

- "Raise awareness of the economic and national security impacts associated with a significant cyber incident
- Highlight available tools and technology with analytical cyber incident response and recovery capability"[181]

Cyber Storm I appears to be attempting to be both an analytical and educational game, and this will be a common thread amongst the Cyber Storm games. Broadly, the goal appears to be exploring the current environment of communication and coordination between the public-private sector, how it fits into the overarching national security agenda, and its impact on the real world. However, it also educates its players on the aforementioned topics, as players are representing entities responsible for establishing real-world coordination efforts. To accomplish this, the game is based on the 'current-day' because it tests the current cyber communication policies, agencies, and norms of interactions at the time. This game fits into the purpose category of understanding the current cyberspace landscape and identifying limitations in the policy.

It places participants, public agency members from the federal and state, within a series of vignettes that were developed with input from industry experts for an overarching cyber threat campaign. Adversaries in the scenarios had three objectives: "disrupt specifically targeted critical infrastructure," hinder governments' ability to respond," and "undermine public confidence."[182] This ranged from targeting energy and transportation, private information databases, and state service systems. The sample provided scenario showcased a state official discovering that the HIPAA database had

[181] National Cyber Security Division.
[182] National Cyber Security Division, 10.

been compromised, correlated with information that other states were having similar cyber incidents and that other state service support systems were non-functioning. These incidents escalated up the ladder, combined with an extortion threat. The Control Cell ran the adversarial team of hackers and created the injects of the cyber incidents.

The achievement list highlights the extensiveness and scale of the cyber exercise and has three key achievements:

- "Tested, for the first time, the full range of cyber-related response policy, doctrine, and communications methodologies that would be required in a real-world crisis"
- "Tested policies and procedures associated with a cyber-related Incident of National Significance, as outlined within the National Response Plan's Cyber Incident Annex"
- "Identified recovery issues that warrant additional review" [183]

For context, The National Response Plan's Cyber Incident Annex is an annex from 2004 that describes the coordination measures to "prepare for, respond to, and recover from cyber-related Incidents of National Significance" which is described as an incident "capable of causing extensive damage to critical infrastructure or key assets."[184] A portion of this is the activation of the IIMG, which according to the National Response Plan, is "a tailored group of senior-level Federal interagency representatives who provide strategic advice to the Secretary of Homeland Security" and the NCRGG which is an "interagency

[183] National Cyber Security Division, 5.
[184] U.S. Government, "Cyber Incident Annex National Response Plan" (U.S. Government, 2004), 1–2, https://www.hsdl.org/?view&did=484571.

forum" of "senior representatives from federal agencies."[185] The plan also lists the communication channels, six channels managed by Homeland Security or the U.S. Computer Emergency Readiness Team (US-CERT), and the roles and responsibilities of the agencies such as the Department of Defense, Department of Homeland Security/Infrastructure Analysis and Infrastructure Protection/National Cyber Security Division, Department of Justice/Federal Bureau of Investigation, Department of Homeland Security/U.S. Secret Service, and Department of State.

The findings section listed eight findings that were based on observations from the gameplay. There needs to be a better understanding from all involved parties of their roles and responsibilities, the responsibilities and level of federal engagement with the activation of the IIMG and NCRP, as well as the formal planning and risk assessment of cyber incidents. Cyber incidents were often not correlated across the public and private sector and treated as individual one-offs, while the more cyber incidents there were, the more difficult response coordination became. Communication, when "synchronized" and "continuous" created a "Common framework for response and information access."

Lastly, there were three suggestions: a "training and exercise program" would improve understanding of cyber response policies, public messaging is critical for information and public reaction in line with the situation, and "processes, tools, and technology – focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios" would improve responses. The report includes a next steps section: the DHS is shifting procedure, policy, and organization, and

[185] Department of Homeland Security, "National Response Plan Brochure," n.d., https://www.dhs.gov/xlibrary/assets/NRP_Brochure.pdf; U.S. Government, "Cyber Incident Annex National Response Plan."

individual participants are working with their organization to create a concept of operations.

Game Analysis

There can be little judgment made on the fidelity of adjudication or game scenario, given the sparseness of the report, which will be another common theme among the Cyber Storm series, and released reports on government wargames in general. This means that readers cannot judge the ecological, internal, or external validity of the game. The internal validity is assumed based on the findings, the external validity for the series is also assumed because the findings and recommendations apply to the real world, and the ecological validity, given the player selection, appears to be relatively representative of the real world. The game offers the first of its kind by testing the communication measures between and within private and public agencies on a large scale, which holds merit because it contributes to a higher level of ecological validity than other representations which may display only the public or private side. The report includes observations that led to the eight findings, allowing the reader to see the thought process behind why those particular findings were developed, which allows for readers to make their judgments as to the accuracy of data analysis.

Given the information provided in the report, it is unclear if the agencies listed in the Cyber Index Annex were represented via players or player roles, which means that the need for a better understanding of their roles and responsibilities could be due to two aspects: players not understanding how to play their assigned roles, or players, representing their real-world agencies, not understanding their agencies' roles and responsibilities in a cyber incident. The first is a problem of game design and role

explanation, and the second is an analysis of a real-world problem. While the report describes that "one of the fundament objectives of the exercise was for key interagency organizations within Federal response infrastructure to exercise their role and responsibilities under the NRP [National Response Plan]," it then states they include the NCRCG and the IIMG, leaving it unclear if the players representing organizations were actual members of their representative agency.[186] Within the exercise, the report cites the successful activation of both organizations, "both compromised of senior representatives from Federal departments/agencies."[187] It is unclear who these representatives are, and if they would correlate seniority-level wise with the actual representatives that would be activated (or if, at that point in time, they were the individuals that would be activated).

Therefore, because the explanation of player roles and responsibilities is not included in the game report, it is unclear whether the need for better explanation stems from game design or a true need for better-defined agency dynamics.

This report is written as a summary of Cyber Storm I, and therefore it only includes 23 pages of the key information: what was the goal, what did the game achieve, what did the game find. However, this creates a reliance on trust and opacity of the process of the game. The sparseness of the report is useful for a sponsor, but not useful for replicability or modeling the next version of the game. The designers for next year, or any other organization that takes on the role of continuing the series, should have access to the full details of game design and data to make sure the 'saturation' of future iterations remains useful. In other words, ensure that future iterations are producing new insights and data.

[186] National Cyber Security Division, "Cyber Storm Exercise Report," 3.
[187] National Cyber Security Division, 4.

Cyber Storm II

Cyber Storm II's goal was "to examine the processes, procedures, tools, and organizations in response to a multi-sector coordinated attack through, and on, the global cyber infrastructure."[188] The objectives were:

- "Examine the capabilities of participating organizations to prepare for, protect from, and respond to the effects of cyber attacks;
- Exercise senior leadership decision making and interagency coordination of incident responses in accordance with national-level policy and procedures
- Validate information sharing relations and communication paths for the collection and dissemination of cyber incident situation awareness, response, and recovery information; and
- Examine the means and processes to share sensitive and classified information across standard boundaries in safe and secure ways without compromising proprietary or national security interests."[189]

The scenario is set in a world where bad actors targeted critical infrastructure, federal entities, and degraded Internet and communications on a global scale. Communication degradation was a key component, with entities on the state and national levels unable to publish or receive information.

Cyber Storm II had the following findings:

---

[188] National Cyber Security Division, "Cyber Storm II Final Report" (Department of Homeland Security, 2008), https://www.cisa.gov/publication/cyber-storm-final-reports.
[189] National Cyber Security Division, 7–8.

"Value of standard operating procedures and established relationships" before and during an attack helped with standardized plans and responses.[190] The standard operating procedures for cyber responses improved significantly after Cyber Storm I for both new and returning players. [191] Physical and cyber interdependencies," as "physical and attacks impact cyber infrastructure and cyber disruptions can have severe physical consequences."[192] Cyber Storm II helped present some participants with their first exercise on a coordinated cyber attack – particularly one where a physical action, like laptop theft, led to cyber risk. [193] "Reliable and tested crisis communication tools" are essential during a crisis, and Cyber Storm II pointed out where there was a lack of tools or inaccessibility.[194] The game also helped with the "clarification of roles and responsibilities" since the first game, increased interaction between public-private entities, retested new and existing cyber response policies, including information sharing, and tested the public side of cyber messaging.[195]

Game Analysis

Cyber Storm II still falls within the purpose of testing existing structures, but it also has a secondary increased focus on communication between cyber experts and non-experts. The report explicitly states that "both public and private sector public affairs players leveraged and enhanced relationships with technical experts" which was "crucial in understanding and communicating."[196] The game itself remarks on growth from the

[190] National Cyber Security Division, 10.
[191] National Cyber Security Division, 10.
[192] National Cyber Security Division, 11.
[193] National Cyber Security Division, 11.
[194] National Cyber Security Division, 12.
[195] National Cyber Security Division, 12–15.
[196] National Cyber Security Division, 15.

first game, which, while sharing the same general overarching goal of evaluating the current state of cyber communication, procedures, and coordination, tries to continue developing the relationships and procedures identified in the previous game. However, there is nothing remarkably different regarding the scenario, player breakdown, or execution described in the report compared to Cyber Storm I. The report is still sparse in descriptive value, lending very little to any potential replication, and cyber is represented on an effects-based model.

The game serves best as an exercise on the current state of cyber communication and coordination to build on the previous iteration, rather than generating any new insights. The report mentions that the game is an "impact analysis of the observations and findings" but "the informational foundation for continuing efforts to assess how those findings translate into steps," which it serves, as the Department of Homeland Security aims to implement the generalized findings into its procedures and encourages the organizations represented in the game to do the same.[197]

Cyber Storm III

Cyber Storm III was a one-sided, seminar-style game from September 27 to October 1, 2020.[198] The exercise goals were: "to examine and enable the plans, capabilities, and procedures necessary to ensure the security of the Nation's broad and interdependent cyber infrastructure" while explicitly relying on the learnings from the past. The exercise objectives were to exercise the National Cyber Incident Response Plan,

[197] National Cyber Security Division, 6.
[198] National Cyber Security Division, "Cyber Storm III Final Report" (Department of Homeland Security, July 2011), 11, https://www.cisa.gov/publication/cyber-storm-final-reports.

the role of the Department of Homeland Security during a cyber crisis, information sharing, and coordination across public-private and international relations.[199]

The scenario was a series of "simulated, targeted attacks resulting from compromises to the Domain Name System (DNS) and the Internet chain of trust"[200] The game focused on "the information technology, communications, energy (electric), chemical, and transportation critical infrastructure sectors."[201] During the game, the Department of Homeland Security had nearly 2000 players, with 100 controllers as ExCon, which ran the white cell support and exercise management. [202] The adversary was an umbrella organization for the cyber crime; it acted as a mercenary for criminal and terrorist groups and was connected to political elites with a strong anti-Western ideology and talented computer engineers.

There were eight scenario targets:[203]

- "Widespread Service Update Compromise" through malware, phishing, logic bombs, and bricking
- "Energy Management System (EMS) Compromise" with a logic bomb and impact to control systems;
- "Chemical and Transportation" that affected the supply chain

[199] National Cyber Security Division, 6.
[200] National Cyber Security Division, 2.
[201] National Cyber Security Division, 5.
[202] National Cyber Security Division, 11.
[203] National Cyber Security Division, 12–13.

- "Federal Scenario" through spearphishing, denial of service attacks, and personal information compromises to disrupt Department of Homeland Security websites and communication
- "International Scenario" that affected Australia's command and control networks for critical infrastructure, a defacement attack on Canada's government IT resources, and a worm attack across several countries that leaked sensitive information
- "DOD/LE/I" which compromised the Defense Department's network through malware
- "PA Scenario" where private companies were hacked and public panic ensued
- "State Scenario" with state networks compromised and personal information exfiltrated

Data was captured through several mechanisms, each player organization had someone that monitored player and outcome developments, after the exercise, there was a post-exercise questionnaire, and several other post-exercise events to discuss specific findings and observations.[204]

The Cyber Storm III had five high-level findings:

1. The National Cyber Incident Response Plan requires more integration into Standard Operating Procedures, response plans, and partner operation plans.[205]

[204] National Cyber Security Division, 11.
[205] National Cyber Security Division, 14.

2. Public-private interaction has been improved but is still marked by a lack of information sharing, role and responsibility uncertainty, and legality and consumer concerns.[206]
3. A common operating picture is needed across all operating entities for situational awareness.[207]
4. The National Cyber Risk Alert System needs more definition for alert thresholds, communication shifts, and recommended actions and incorporation into standard operating procedures.[208]
5. Strategic public communication is critical for public confidence and coordinated cyber response.[209]

Game Analysis

The game is an exercise of the National Cyber Incident Response Plan, a plan that began development in 2008 under the Bush administration, with a draft produced in 2009.[210] The version that the Cyber Storm III is referring to is likely the 2010 Interim Version, published right before the game began in late September 2010.[211] This draft version was given to participants in preparation for the game.[212] The exercise includes

---

[206] National Cyber Security Division, 16.
[207] National Cyber Security Division, "Cyber Storm III Final Report."
[208] National Cyber Security Division, 19.
[209] National Cyber Security Division, 20.
[210] Robert Dix Jr, "A National Cyber Event Requires Clarity for Roles and Responsibilities," SIGNAL Magazine, May 28, 2015, https://www.afcea.org/content/Blog-national-cyber-event-requires-clarity-roles-and-responsibilities.
[211] Department of Homeland Security, "Draft National Cyber Incident Response Plan" (Department of Homeland Security, September 2010), https://www.cisa.gov/uscert/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf.
[212] National Cyber Security Division, "Cyber Storm III Final Report," 15.

more follow-on events than in previous Cyber Storms, which shows an increased commitment to analytical value and implementation.[213]

Cyber Storm III marked a change in report writing, with more specificity in regards to the scenario and specific attacks. The adversarial attacks had causality alongside an effects-based description and played along with a core scenario with different targets rather than vignette-style separated scenarios. The differing targets allowed participants to have scenarios more tailored to their real-world organization, and understand how specific sectors and industries fit into overall national goals. The inclusion of international country coordination is the same as in previous Cyber Storm games but remains limited – as noted by the lack of learnings or findings on international coordination in the report. Although a wide-scale attack occurring within a limited timespan across multiple sectors remains unrealistic, the breakdown into individualized targeted attacks gives players a greater sense of plausibility because participants can focus on their organization's response to a realistic attack, and then understand how it fits into a worst-case scenario of a global effort. The report continues to not include outcome results, which is likely due to the carry-over focus on deliberative data rather than outcome data carried over from previous Cyber Storm. However, without including the participants' instructions as to their capabilities, it is also difficult to verify the findings as

Cyber Storm IV

Cyber Storm IV marked a change from other versions because it encompassed 15 building block exercises rather than one all-encompassing game run from 2011 to 2014. The objectives of Cyber Storm IV were to: improve the processes and procedures of the

[213] National Cyber Security Division, 11.

National Cyber Incident Response Plan, exercise the role of the Department of Homeland Security, and communication and coordination of private and public stakeholders.[214] The fifteen events included larger tests on the National Cyber Incident Response Plan specifically, Public Affairs, State coordination, individual state tests, international member nation coordination, and infrastructure response on the local level.[215] Out of the fifteen exercises, only four are operations-based, while the rest are discussion-based table-top exercises or seminars. There were four trends observed: Cyber response and operating plans need clear roles, responsibilities, procedures, and training must accompany plans to be understood.[216] Information sharing mechanisms and content remained uncertain, and resource identification and allocation were hampered by knowledge.[217] Cybersecurity training and awareness are important across all stakeholders.[218]

Games Analysis

There is very little analysis that can be done, given the lack of information regarding the specificity of the exercises. The two things of note are the state-specific tests and the testing of the National Cyber Incident Response Plan. The former gives states a chance to understand how they fit into the national response – helpful in the case that a cyber attack originates in one of the states that had an individualized exercise.

---

[214] National Cyber Security Division, "Informing Cyber Storm V: Lessons Learned from Cyber Storm IV" (Department of Homeland Security, June 2015), 1, https://www.cisa.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf.
[215] National Cyber Security Division, 3–4.
[216] National Cyber Security Division, 4.
[217] National Cyber Security Division, 5–6.
[218] National Cyber Security Division, 7.

Cyber Storm IV continues to test the same National Cyber Incident Response Plan, which then raises the question: because the plan has not been updated, is this test useful for generating new recommendations? Based on the findings, which are less specific than the Cyber Storm III findings, Cyber Storm IV exercises only reconfirmed previous trends of needing better information sharing, roles and responsibilities, and confusion over coordination.

Cyber Storm V

Cyber Storm V did not have a new cyber framework to evaluate, so its exercise goal was to: "strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure." The exercise objectives are very similar to the goal, to "continue to exercise coordination mechanisms, information sharing efforts, development of share situational awareness, and decision-making procedures," "evaluate relevant policy, statutory, and fiscal issues," "access the role, functions and capabilities of the DHS and other government entities" with over 1200 participants.[219]

The scenario was based around "common protocols and services" such as routing methods, the Domain Name System, and the Public Key Infrastructure, which impacted a variety of private and public sectors including "Information Technology, Communications, Healthcare and Public Health, and Commercial Facilities."[220] This

[219] National Cyber Security Division, "Cyber Storm V: After Action Report" (Department of Homeland Security, July 2016), 1, https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.
[220] National Cyber Security Division, 1–2.

produced four high-level findings that mirror Cyber Storm III and IV: a national level framework understood by stakeholders would have improved the cyber incident response, information sharing challenges, such as channels, speed, and liability, still exist, and there is more awareness of the role and responsibilities of government-specific entities like the Department of Homeland Security.[221] The data collection and run were similar to Cyber Storm III with individual exercise planning team individuals located at the organizations' home base that reported on the scenario and player interaction, and a questionnaire after gameplay.[222] Cyber Storm V also included follow-up events, similar to Cyber Storm III. Cyber Storm V, for the first time, included the Healthcare and Public Health Sector and the Retail Sector, which allowed for greater private sector coordination and buy-in.[223] As Cyber Storm V follows the same format and report structure as Cyber Storm III, with less specificity in regards to the scenario and adversary, the same criticisms and concerns apply.

Cyber Storm VI

The goal of Cyber Storm VI in 2018 was the same as Cyber Storm V: "Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure."[224] However, the objectives return to the National Cyber Incident Response Plan and the 2016 version, which includes exercising the National Cyber

---

[221] National Cyber Security Division, 2.
[222] National Cyber Security Division, 15.
[223] National Cyber Security Division, 2.
[224] National Cyber Security Division, "Cyber Storm VI: After Action Report" (Department of Homeland Security, 2018), 1, https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

Incident Response Plan, information sharing, the role of the Department of Homeland Security, and public-private coordination.[225] Cyber Storm 2020's participant amount, 2000, was almost double that of Cyber Storm V, encompassing a much broader participant pool.[226] The scenario for this iteration of the game was based on a "vulnerability in an embedded microprocesses used in a wide variety of traditional and non-traditional IT devices" which resulted in a national level failure: "cars being unable to start, robots on factory floors failing, and IoT devices being leveraged for attacks on corporate or government networks."[227] The chip vulnerabilities were spread across all traditional and non-traditional IT devices in industries like "robotics, building automation, automotive, aviation, industrial control systems, and computers."[228] The data collection and game process ran the same as Cyber Storm V, with local and centralized exercise teams that observed participant interaction and scenario development. There were surveys for participants for feedback, and after-action events similar to the last Cyber Storm game as well.[229]

There were four main findings:

"Finding 1: The cyber attack landscape continues to expand. Attacks that impacted non-traditional IT devices, such as operational technology, highlighted gaps in people, process, and technology; altered the nature of the cyber incident response lifecycle; and emphasized the need for specialized planning and response considerations that support a more comprehensive view of threats.

---

[225] National Cyber Security Division, 2.
[226] National Cyber Security Division, 5.
[227] National Cyber Security Division, 3.
[228] National Cyber Security Division, 8.
[229] National Cyber Security Division, 21.

Finding 2: Traditional and social media continue to drive awareness of cyber incidents, while also becoming an increasingly significant component of the response. The ability to quickly and effectively engage with customers, stakeholders, and the public; promote accurate information over rumor or misinformation, and support efforts to minimize negative brand impact contribute to the overall response.

Finding 3: The National Cyber Incident Response Plan provides a framework for federal coordination but provides for limited linkages to critical infrastructure and the private sector in the early phases of response. This gap creates uncertainty among and within critical infrastructure sectors and may lead to delays or inconsistencies in response .Finding 4: Trusted and established information sharing paths proved to be the most effective during exercise play. Participants who understood their available resources both internally and externally could verify and share data more effectively."[230]

Game Analysis

Cyber Storm VI's scenario showed a new method of cyberthreat, through physical microprocessors, and focused on processor compromise with more kinetic effects on civilian and private infrastructure like factories and cars. This marks a change in the Cyber Storm scenarios in past years, and also creates an overarching theme of microprocessor exploits as the causal mechanism, rather than the varied intrusion methods in past years. This allows returning participants to grapple with a new problem and brings to light vulnerabilities with a national-level impact.

The game also tests the new National Cyber Incident Response Plan. The 2016 draft version of the National Cyber Response plan, released on September 30, 2016, refers to

[230] National Cyber Security Division, 3–4.

revisions from "large scale cyber exercises such as the Cyber Storm series," and the final version was published in December 2016.[231] The game is exercising the December 2016 version, and the findings note that there needs to be more linkage between the public-private sector, particularly in the earlier stages of the game.

The same report structure is used without participant capability descriptions or an outcome analysis, and therefore the game's fidelity and representation of cyber cannot be analyzed.

Cyber Storm 2020

The goal of Cyber Storm 2020 was to "strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure."[232] The game was sponsored by the Cybersecurity and Infrastructure Security Agency, supported by Booz Allen Hamilton, which currently has a September 2020-2024 contract with the Department of Homeland Security for the yearly development of Cyber Storm.[233] The objectives of Cyber Storm 2020 were to "Examine the implementation and effectiveness of national cybersecurity plans and policies; Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem

---

[231] Department of Homeland Security, "Draft National Cyber Incident Response Plan" (Department of Homeland Security, September 30, 2016), 1, https://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf.

[232] CISA, "Cyber Storm 2020: After-Action Report" (Cybersecurity and Infrastructure Security Agency, August 2020), 3.

[233] "CONTRACT to BOOZ ALLEN HAMILTON INC. | USAspending," accessed November 17, 2021, https://usaspending.gov/award/CONT_AWD_70RCSA20FR0000085_7001_GS00Q14OADU108_4732.

during a cyber incident; Reinforce public and private partnerships and improve their ability to share relevant and timely information; and Exercise communication aspects of cyber incident response to refine and mature communications strategies."[234] Compared to previous Cyber Storms, the industry was present in larger numbers in Cyber Storm 2020, doubling the number of industry partners and sectors and greater incorporation into the wargame since the previous year.

Cyber Storm 2020 played in a 'choose-your-own-scenario"-esque set-up, where the base scenario placed "two nation state-level adversaries" that cooperated to utilize DNS (Domain Name System), CA (Certificate Authorities), and BGP (Border Gateway Protocol) vulnerabilities to attack U.S. and abroad government and private sector targets "with the intent of compromising the confidentiality, integrity, and availability of their systems and data."[235] Ransomware attacks were a key element of gameplay. Participants were able to customize their scenario from a series of eight vignettes: decoy code, phishing campaigns, malicious site redirection, denial of service, BGP hacking, PII exfiltration and dumping, a chain of trust exploitation, and adapt it to their unique network, structure, and business. The participants then collaborated to identify the cyber source, create a response plan, share information, and update strategies."[236]

Data collection and analysis relied mainly on participant surveys, stakeholder lessons learned, and observations recorded, leading to five high-level exercise findings. "Finding 1: CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the internet.

---

[234] CISA, "Cyber Storm 2020: After-Action Report," 3.
[235] CISA, 4.
[236] CISA, 11.

Finding 2: The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine support activities.

Finding 3: In increasingly distributed working environments, some organizations found that distributed response could delay coordination and extend response timelines.

Finding 4: Broad information sharing is critical to recognizing a coordination campaign and CISA has an opportunity to play a proactive facilitating role.

Finding 5: Successful incident response requires planned, whole-of-organization coordination."[237]

Game Analysis

Cyber Storm 2020 was sponsored by the Cybersecurity Infrastructure and Security Agency, CISA, for the first time. CISA was created on November 16, 2018, and therefore not included in previous iterations of the game, although all the Cyber Storm material is now hosted on their site.[238] During the game, participants were able to exercise their technical expertise by trying to "understand attack origins, potential impacts/spread, the vulnerability exploited, and how to contain and fix it," leading to an emphasis on "the importance of two-factor authentication (2FA)," as well as the value of crisis playbooks. However, the stress-testing value is something that could come from individual penetration testing that likely also will be more targeted for the individual organization without participants being able to tailor how exactly they will be attacked.

Participants were also able to test the "incident severity schema… to assess and communicate incident impacts" which holds significant value in the testing of the CISA

[237] CISA, 13–18.
[238] CISA, "Cyber Games | CISA," accessed April 5, 2022, https://www.cisa.gov/cybergames.

and NCIRP National Cyber Incident Scoring System. However, the observation from this remains limited: "Players observed that impacts across multiple sectors and the potential risk environment likely warranted higher aggregate severity levels than the individual incident scores."[239] This is an actionable item that is not reflected in a change in the cyber scoring system, which may be a result of needing additional testing to change the framework, but may also point to a lack of impact of cyber wargames.

In summary, stakeholder recommendations suggested that organizations should continue to "develop a cyber incident response playbook… exercise their cyber incident response capabilities and processes against a variety of scenarios… ensure incident response plans consider both the communicative and physical challenges of the distributed professional environment…ensure clear unity of command," and include public relations, legal, and leadership teams as well as pre-approved messaging before cyber incidents.[240] CISA should also regularly examine processes and resources for stakeholder engagement during and after incidents for future learning, and utilize cross-sector collaboration and information sharing for broad public incident reporting. The benefit of focusing on CISA is creating a guideline for the organization, a relatively new one, to understand how it currently fits into the federal infrastructure and how it can improve in the future, which is unique to Cyber Storm 2020. Crisis communication organizations have begun developing "Ransomware Playbooks" for corporations that lay out, individualized to the company, response plans, pre-drafted messaging, timeline of recommendation for reporting to CISA and the FBI. There are recent concerns that

[239] CISA, "Cyber Storm 2020: After-Action Report," 15.
[240] CISA, 13–18.

organizations have *never* considered a possibility until the rise of ransomware and increased cyberattacks, such as, what happens when traditional communication lines are entirely fried or inaccessible? Lisa Buery-Russo, Acting Deputy Associate Director for Exercises at CISA, noted that the "exercise highlighted the value of CISA and those roles that we carry out for the broader cyber community."[241]

Based on the findings and recommendations, Cyber Storm 2020 appears to just be a large-scale exercise reminding participants that cyber security and communication cross-sector with clients, other companies, and the public sector is critical. However, the value of Cyber Storm 2020 appears to be in three main aspects: (1) Testing the CISA cyber plan, (2) Acting as a wake-up call for the difficulties of information flow and coordination internally and externally, (3) Raising awareness about coordination with CISA, given the newness of the organization. The need to run this on a large scale is specifically for the inclusion of CISA, as many of the findings and actionable recommendations are realizations that could have come from individual corporate wargames and exercises, or re-iterate previous Cyber Storms.

[241] Lisa Beury-Russo, Takeaways from the Cyber Storm exercise, August 23, 2020, https://govmatters.tv/takeaways-from-the-cyber-storm-exercise/.

Cyber Storm Series Analysis[242]

	I: 2006	II: 2008	III: 2010	IV: 2011-2014	V: 2016	VI: 2018	2020	2022
Goals and Objectives	Interagency coordination through the National Cyber Response Coordination Group (NCRCG) pursuant to the Cyber Annex to the National Response Plan; Identification of policy issues that affect response and recovery; Identification of critical information sharing paths and mechanisms among public	Examine the capabilities of participating organizations to prepare for, protect from, and respond to the effects of cyber attacks; Exercise senior leadership decision making and interagency coordination of incident responses in accordance with national level policy and procedures; Validate information sharing relationships and	Exercise and enable the plans, capabilities, and procedures necessary to ensure the security of the Nation's broad and interdependent cyber infrastructure Leverage past and present efforts, initiatives, resources, and findings Exercise the NCIRP Examine the role of DHS in a global cyber event Focus on information sharing issues (e.g.,	Identify, exercise, and foster the improvement of processes, procedures, interactions, and information sharing mechanisms that exist, or should exist, under the draft National Cyber Incident Response Plan (NCIRP) Examine the role of DHS and its associated components during a global cyber event Exercise coordination mechanisms,	Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure Continue to exercise coordination mechanisms, information sharing efforts, development of shared situational awareness, and decision-making	Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure. Exercise Objectives: Exercise the coordination mechanisms and evaluate the effectiveness of the National Cyber Incident Response Plan (NCIRP) in	Examine the implementation and effectiveness of national cybersecurity plans and policies; Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem during a cyber incident; Reinforce public and private partnerships and improve their ability to share relevant and timely information;	Examine the effectiveness of national cybersecurity plans and policies Explore the roles and responsibilities during a cyber incident with potential or actual physical impacts Strengthen information sharing and coordination mechanisms used during a cyber incident Foster public and private partnerships and improve their ability to share relevant and timely

[242] CISA, "Cyber Storm 2020: After-Action Report"; National Cyber Security Division, "Cyber Storm VI: After Action Report"; National Cyber Security Division, "Cyber Storm V: After Action Report"; National Cyber Security Division, "Informing Cyber Storm V: Lessons Learned from Cyber Storm IV"; National Cyber Security Division, "Cyber Storm III Final Report"; National Cyber Security Division, "Cyber Storm II Final Report"; National Cyber Security Division, "Cyber Storm Exercise Report."

	and private sectors; and Identification, improvement, and promotion of public and private sector interaction in processes and procedures for establishing situational awareness; supporting public and private sector decision making; communicating appropriate information to key stakeholders and the public; and planning and implementing appropriate response and recovery activities. Secondary goals of the exercise included: Highlighting specific tools	communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information; and Examine the means and processes to share sensitive and classified information across standard boundaries in safe and secure ways without compromising proprietary or national security interests.	requirements, classified/tear-line, information condition/alert levels, thresholds, response roles and responsibilities, authorities) Examine coordination and decision-making procedures/mechanisms across the constituency (federal, state, private sector, international) Practically apply elements of past or ongoing initiatives, findings from past exercises, and other related cybersecurity efforts	information sharing efforts, development of shared situational awareness, and decision-making procedures of the cybersecurity community (Federal, state, private-sector, and international) during cyber events	procedures of the cyber incident response community during a cyber event Evaluate relevant policy, statutory, and fiscal issues that govern cyber incident response authorities and resource prioritization Provide a forum for exercise participants to exercise, evaluate, and improve the processes, procedures, interactions, and information sharing mechanisms within their organization or community of interest Assess the role, functions, and	guiding response; Assess information sharing to include thresholds, paths, timeliness, usefulness of information shared, and barriers to sharing both internally and externally within the cyber incident response community; Continue to examine the role, functions, and capabilities of DHS as the Department coordinates with impacted entities during a cyber event; and Provide a forum for exercise participants to exercise, evaluate, and improve the processes,	Exercise communication aspects of cyber incident response to refine and mature communications strategies.	information across partners

	and analytical capabilities that may be used in preparation for, response to, and recovery from cyber incidents; and Raising awareness of the economic and national security impacts associated with a significant cyber incident.				capabilities of DHS and other government entities in a cyber event	procedures, interactions, and information sharing mechanisms within their organization or community of interest		
Findings	Finding 1: Interagency Coordination. While the Interagency Incident Management Group (IIMG)1 and National Cyber Response Coordination Group (NCRCG) activated and interacted	Finding 1: Value of Standard Operating Procedures (SOPs) and Established Relationships. Preparation and effective response is significantly enhanced by established and coordinated SOPs	The NCIRP provides a sound framework for steady-state activities and cyber incident response; however, the supporting processes, procedures, roles, and responsibilities outlined in the Plan require maturity. To truly serve as	Trend 1: Cyber Response and Operating Plans Cyber response and operating plans are used by both public and private organizations as guiding mechanisms for cyber incident response. Participants generally	Finding 1: A current, national-level plan or framework that has widespread buy-in, adoption, and integration would have formalized and optimized cyber incident response during CS V. Finding 2: Challenges	Finding 1: The cyber attack landscape continues to expand. Finding 2: Traditional and social media continue to drive awareness of cyber incidents, while also becoming an increasingly significant	Finding 1: CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet Finding 2: The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine	

	constructively during the exercise, further refinement is needed for operations and coordination procedures. Finding 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities. Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified Finding 3: Correlation of Multiple Incidents between Public and	and existing relationships in the cyber response community. Finding 2: Physical and Cyber Interdependencies. Cyber events have consequences outside the cyber response community, and non-cyber events can impact cyber functionality Finding 3: Importance of Reliable and Tested Crisis Communications Tools. Tools and related methods developed and deployed for handling crisis communications need further refinement and enhancement. Finding 4: Clarification of Roles and Responsibilitie	the framework for national-level cyber incident response, NCIRP concepts need to be further integrated into supporting Standard Operating Procedures (SOPs) and Concepts of Operations (CONOPS), complementary response plans, and corresponding partner operating procedures. Finding 2 Cyber response collaboration among private-sector companies has advanced because of targeted initiatives and understanding of mutual benefit. Although	agreed the ability to effectively leverage cyber incident response plans promotes coordination, awareness, and recovery in the event of an enterprise-wide cyber incident. Trend 2: Information Sharing and Communications While the Department and the cyber incident response community are improving their respective abilities to share information needed to make decisions during cyber incidents, the issue remains a challenge requiring continued	around information sharing – thresholds, paths, speed of sharing, and liability issues – still exist and need targeted attention. Finding 3: CSV players displayed increased awareness of the NCCIC's role in information sharing and shared situational awareness and increasingly looked to DHS, the NCCIC, and US-CERT to coalesce information and provide reporting back out. DHS and the NCCIC should build upon this and continue to improve their processes, procedures,	component of the response. Finding 3: The National Cyber Incident Response Plan provides a framework for federal coordination but provides for limited linkages to critical infrastructure and the private sector in the early phases of response. This gap creates uncertainty among and within critical infrastructure sectors and may lead to delays or inconsistencies in response. Finding 4: Trusted and established information sharing paths proved to be the most effective during exercise play.	supporting activities Finding 3: In increasingly distributed working environments, some organizations found distributed response could delay coordination and extend response timelines Finding 4: Broad information sharing is critical to recognizing a coordinated campaign and CISA has an opportunity to play a proactive facilitating role Finding 5: Successful incident response requires planned, whole-of-	

	Private Sectors. Finding 4: Training and Exercise Program. Finding 5: Coordination Between Entities of Cyber Incidents. Finding 6: Common Framework for Response and Information Access. Finding 7: Strategic Communications and Public Relations Plan. Public messaging must be an integral part of a collaborated contingency plan and incident response. Finding 8: Improvement of Processes,	s. Substantial improvements since Finding 5: Increased Non-Crisis Interaction. Regular, non-crisis related communications and interaction within the cyber response community through established means would solidify communications paths, strengthen relationships and clarify organizational cyber incident response roles. Finding 6: Policies and Procedures Critical to Information Flow. Finding 7: Public Affairs Influence During Large-Scale Cyber	public–private interaction around cyber response is continually evolving and improving, it can be complicated by the lack of timely and meaningful shared situational awareness; uncertainties regarding roles and responsibilities; and legal, customer, and/or security concerns. Finding 3 To foster common awareness and support decision-making during a crisis, development, distribution, and maintenance of shared situational awareness—sometimes referred to as a	focus. Efforts by public and private stakeholders to develop operational relationships, formalize information sharing procedures and establish command and control structures prior to an incident contribute to improved information sharing and communication during cyber incident response and enhance the collective ability to respond. Trend 3: Resource Identification and Allocation the ability to effectively leverage internal and external resources to improve cyber	and overall capabilities. Finding 4: As first-time Cyber Storm exercise participants, the Healthcare and Public Health Sector and the Retail Subsector both observed the value of increased coordination within the sector, expanded information sharing across affected sectors, and the value of more formalized coordination and reporting mechanisms through entities such as ISACs or ISAOs.	Participants who understood their available resources both internally and externally could verify and share data more effectively.	organization coordination	

	Tools, and Technology.	Incidents. During a cyber event, public affairs can be used to educate and inform the public through clear, actionable information validated by technical experts and entities such as Sector Coordinating Councils (SCCs) and sector Information Sharing and Analysis Centers (ISACs). Finding 8: Greater Familiarity with Information Sharing Processes. Exercise findings suggest the value of continued effort devoted to training, use	common operating picture (COP) or, in this case, a cyber COP—across the community is a critical requirement. Finding 4 The National Cyber Risk Alert Level (NCRAL) is intended to inform preparedness, decision-making, information-sharing requirements, and cyber incident management activities Finding 5 The Government, the private sector, and the general public rely on timely, accurate, and actionable public and strategic communicatio n to manage	incident response capabilities. Trend 4: Cybersecurity Training, Awareness, and Education Awareness of cyber threats, attack vectors, and recent incidents can be improved across the cybersecurity stakeholder spectrum.				

		of existing procedures, and familiarity with designation authorities to allow more rapid response and information flow through various mediums.	threats to their networks.					

The March 2022 Cyber Storm exercise does not have a write-up, but the objectives of the game become shorter, as the sponsor narrows down the exercise goals into four key trends seen across all Cyber Storm games: testing national cybersecurity plans, roles and responsibilities, information sharing and coordination, and public-private partnerships.[243] There is no one national cybersecurity plan specified in the goal, which likely makes the game design more difficult but is reflective of a lack of a new National Cyber Incident Response Plan since the 2016 version.

Cyber Storms (except for IV) are meant to be a large, complicated games, however, if the purpose of Cyber Storm is to see how "stakeholders from the public and private sectors and international partners would collectively respond to a widespread cyber attack," the division of the vignettes raises the question of how collaboration was supposed to work if every participating organization was hit with a different, unique attack tailored to them in some versions of the games. That being said, the private-public sector interaction for individual agencies appears to be at the forefront of the game design, as well as eventual large private sector collaboration, particularly during games that test the National Cyber Incident Response Plan variants. [244]

Cyber Storms' value is not in its findings and recommendations, because the findings derived from the games appear to be findings non-unique to the game itself, or without any particularly new insight regarding the cyber domain. To return to the findings listed previously, the main value appears to be one of 'stress the 'long-standing' vulnerabilities of the internet. Given the level of participants, it is highly unlikely that

[243] CISA, "Cyber Storm VIII: National Cyber Exercise," March 2022, https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise.
[244] Beury-Russo, Takeaways from the Cyber Storm exercise.

these private or public sector participants are unaware that information sharing and planned responses are critical to responding to cyber attacks, and therefore the report turns to the observations, which also include potential lessons learned for the participants and the stakeholder recommendations.

The largest criticism across all Cyber Storms is that the findings are too generalized and repetitive, at least in the reports. Almost all the reports test the national cybersecurity response infrastructure, the necessity of planning, coordination, information sharing, the definition of roles and responsibilities, relationships between the public and private sector, and operating procedures, and almost all findings include that these are improving but need more improvement, seen in the color-coding. This could be due to the framing of Cyber Storm as a quasi-analytical educational game, the concern brought up in the Cyber Storm I analysis.

Therefore, the impact of the game is one for the players of the game, as a national-level exercise where participants, including the sponsor who is represented, gain knowledge on how to respond to a large-scale cyber attack, rather than deriving any particularly insightful new information in how this response occurs. There is an actionable impact from the Cyber Storm series on national frameworks for cyber communication, specifically the National Cyber Incident Response Plan. The 2010 version was tested in Cyber Storm III, and findings from Cyber Storm III appear to have affected the updated 2016 version.

The 2010 Interim Version Table of Contents (98 Pages, 29 before Appendix)[245]	The 2016 Final Version Table of Contents (68 Pages, 34 before Appendix)[246]
1. Introduction a. Purpose b. Scope 2. National Concept of Operations a. Common Operational Picture b. Centralized Coordination, Decentralized Execution c. General Roles and Responsibilities for Cyber Incidents d. Supported and Supporting Relationships 3. Organization of the National Cybersecurity and Communications Integration Center a. National Cybersecurity and Communications Integration Center Organization During Steady State b. Organization During a Significant Cyber Incident 4. Actions of the Cyber Response Cycle a. Coordination and the Common Operational Picture b. Prevent and Protect c. Analyze d. Respond	1. Executive Summary 2. Introduction 3. Scope a. Guiding Principles 4. Relationship to National Preparedness System 5. Roles and Responsibilities a. Concurrent Lines of Effort b. Threat Response i. Private Sector ii. State, Local, Tribal, and Territorial Government iii. Federal Government c. Asset Response i. Private Sector ii. State, Local, Tribal, and Territorial Government iii. Federal Government d. Intelligence Support i. State, Local, Tribal, and Territorial Government ii. Federal Government e. Affected Entity's Response i. Cyber Incidents Involving Personally Identifiable Information 6. Core Capabilities a. Access Control and Identification Verification b. Cybersecurity c. Forensics and Attribution d. Infrastructure Systems e. Intelligence and Information Sharing f. Interdiction and Disruption g. Logistics and Supply Chain Management

[245] Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 2010.

[246] Department of Homeland Security, "National Cyber Incident Response Plan" (Department of Homeland Security, December 2016), https://www.cisa.gov/uscert/ncirp.

e. Resolve

5. Universal Roles and Responsibilities
    a. Preparedness
    b. Cyber Incident Response
    c. Short-Term Recovery

Appendix

A. National Cyber Response Framework Cyber Incident Annex
B. Department of Homeland Security Roles and Responsibilities
C. Department of Defense Roles and Responsibilities
D. Department of State Roles and Responsibilities
E. Intelligence Community Roles and Responsibilities
F. Department of Justice Roles and Responsibilities
G. All Federal Department and Agency Roles and Responsibilities
H. State, Local, Tribal, and Territorial Roles and Responsibilities
I. Private Sector Critical Infrastructure and Key Resources Roles and Responsibilities
J. Executive Office of the President
K. National Cyber Risk Alert Level System
L. Authorities
M. Definitions
N. Organizations
O. Acronym List

h. Operational Communications
i. Operational Coordination
j. Planning
k. Public Information and Warning
l. Screening, Search, and Detection
m. Situational Assessment
n. Threats and Hazards Identification

7. Coordinating Structures and Integration
    a. Coordinating Structures
        i. Private Sector
        ii. State, Local, Tribal, and Territorial Government
        iii. International
    b. Operational Coordination During a Significant Cyber Incident
        i. Determination of Incident Severity
        ii. Enhanced Coordination Procedures
        iii. Cyber UCG
        iv. Information Sharing During Cyber Incident Response
8. Conclusion

Annex

A. Authorities and Statutes
B. Cyber Incident Severity Schema
C. Cyber Incident Severity Schema/National Response Coordination Center Activation Crosswalk
D. Reporting Cyber Incidents to the Federal Government
E. Roles of Federal Cybersecurity Centers
F. Core Capabilities and Critical Tasks
G. Developing an International Cyber Incident Response Plan
H. Core Capability/NIST Cybersecurity Framework

	I. Additional Resources J. Acronym List

In Cyber Storm III, under the findings that the National Cyber Incident Response Plan required more development, one of the key observations was that players "did not have a clear understanding of the organizations involved, their relative roles and responsibilities, or how to interact most beneficially within the community… [including] the type of information to share and the format for submission."[247] This may have impacted the additional section in the 2016 version-specific on information sharing, and the change in structure from the roles and responsibilities of individual entities being placed in the Appendix in the 2010 version to the separation of roles and responsibilities by responsibility first, then how entities should go about it (for threat response, asset response, intelligence support, and entity response).[248]

Cyber Storm III also reiterated the need for further coordination, common operating picture methods, and sharing of information, and while this is expressed in the 2010 interim draft, it is reformatted and expanded upon in the 2016 version, with a section dedicated to situational awareness under core capabilities, and an entire section on coordination alone.[249] There is no updated version of the 2016 final draft based on the findings from Cyber Storm VI, and the language in the games afterward switches to testing 'cyber response plans' rather than a specific national framework.

[247] National Cyber Security Division, "Cyber Storm III Final Report," 16.
[248] Department of Homeland Security, "Draft National Cyber Incident Response Plan," September 2010; Department of Homeland Security, "National Cyber Incident Response Plan."
[249] National Cyber Security Division, "Cyber Storm III Final Report."

The framing of Cyber Storm as trying to analyze and educate, rather than just test the existing state of current systems, also affects its report structure. While each report includes the observations that lead to its findings, to apply its findings within the real world or demonstrate external validity, it should also include specificity as to how participants were allowed to interact with the environment, which was missing from all the reports. The Cyber Storm series is a useful wargame for creating an environment and platform to exercise current structures to educate participants, but its analytical value is low. However, creating a publicly accessible report is also useful, despite the shortness of the report, for informing other private organizations that did not directly participate in Cyber Storm.

Global Title X Series

Global Title X Series 10

The Global Title X Series 10: Global Maritime Partnership Game is the first available Global X, declassified game in the US Naval War College repository, although the Global Title X series is run annually.[250] While this specific game did not explicitly mention cyber, the subsequent two other available games, which do incorporate the cyber domain, offer the opportunity to see how a sequential game designed by the same designers, with the same sponsor, developed.[251]

This game, sponsored by the Navy, had the overarching research question:

[250] Don Marrin et al., "Global Title X Series '10: Global Maritime Partnership Game," Game Reports (U.S. Naval War College, 2010), https://digital-commons.usnwc.edu/game-reports/12.

[251] For this reason, only the general purpose and design of the game, as well as potential improvements will be noted. For game results, please refer to the full game report.

"Based on the catalysts to instability derived from the participants, what were the impediments and proposed collaborative solutions to forming effective partnerships at the sub-regional, regional, and cross-regional levels from both United States and international perspectives?"[252]

There were four specific objectives: Identify (1) "maritime regional and cross-regional challenges.. from both international and U.S. perspectives" and (2) "broad-based partnership requirements… [that] enable Maritime Domain Awareness (MDA) to counter these challenges." Provide a space for participants to (3) "explore and appreciate the complexities of establishing and maintaining effective maritime partnerships" and (4) "familiarize themselves with… current technological research and innovations in Maritime Domain Awareness."[253]The participants incorporated "83 participants from 46 countries," from both civilian and military backgrounds with MDA subject matter expertise, and its development was based on the new maritime strategy, *A Cooperative Strategy for 21st Century Seapower.*[254] Player interaction was in-person, in a three-phase game. The first section was looking at the present situation, identifying issues and current solutions; the second phase was to develop their solutions in small cells of 10-12 (design parameters being 7-14) and present them through panels to the broader audience; the third was the conclusion of the game and an MDA technology symposium.[255] Data was collected through environmental recorders, player surveys, and group products and

[252] Marrin et al., "Global Title X Series '10: Global Maritime Partnership Game," 1.
[253] Marrin et al., 1.
[254] Marrin et al., 1–7.
[255] Marrin et al., 11.

analyzed via content analysis, grounded theory, and data visualization (via tools like i2 Text Chart and the Analyst's Notebook).[256]

The game was a "single-sided seminar-style analytical game with a control cell" "as a catalyst for inductively-generated knowledge."[257] The American participants had to develop recommendations as a part of the game design that were actionable, and this followed three general categories of "organize, train, and equip" at the "sub-regional, regional, or cross-regional levels."[258] Limitations of game design noted that "no inferentiality or generalizability can be assumed based on the results of this game" and that there were potential issues that affected the internal and external validity.[259] The authors of this report and game note that "games are not experiments" and therefore, a game is representative only of that specific subset of players making those specific actions – the validity of a game (the authors describe internal validity as the ability to infer cause-and-effect from the game data and external validity as the game results reflecting the external world) is too low for generalizability. The validity was restricted by the data collection and analysis, as well as the international aspect of the participants with English being used as a second language. [260]

However, the game did help develop new insights and theories that can be expanded upon in future research, and the authors include a section on suggested future

---

[256] Marrin et al., 11–12.
[257] Marrin et al., 144–124.
[258] Marrin et al., 18.
[259] This is a common theme among the Global Title X Series, as well as the beliefs of the authors of this report and the designers of the game – that the decisions and conclusions reached within a certain game are player-specific, and game analysis should be wary of claiming to be broadly generalizable. Marrin et al., 20.
[260] Marrin et al., 21.

games for research with proposed objectives.[261] The game report is extensive and follows a clear pattern of overview, game design, analysis and results, and then lessons learned and recommendations. The demographics of the participants are broken down, and the appendix includes the background, the schedule, and each cell's produced material of impediments to partnerships and potential solutions. It also includes further details on game design and mechanics.

Global Title X Series 13

Global Title X is built on the annual Title 10 game, although the 2012 wargame was not released for public distribution. The 2012 game concluded that "current command and control (C2) structures at the operational level of war may be inadequate to effectively execute cross-domain operations as envisioned by the [Air-Sea Battle (ASB)] concept." [262] This led to the research question driving the new 2013 game, sponsored by the Navy: "Which of the three candidate C2 systems is best suited to command and control combined forces engaged in cross-domain operations in a high-intensity A2/AD [Anti-Access/Area-Denial] environment, and why?" [263]

The Global 2013 project was a three-part process: "an online C2 Requirements Workshop (development of C2 criteria and conditions), a C2 Options Development Workshop (development of candidate C2 systems), and the Capstone Event (examination of the

[261] Marrin et al., 28.
[262] Don Marrin, Walter Berberick, and Wargaming Department, "Global Title X Series '13: Game Report," Game Reports (U.S. Naval War College, 2014), 2, https://digital-commons.usnwc.edu/game-reports/13/.
[263] Marrin, Berberick, and Department, 2.

candidate C2 systems) where three C2 systems were chosen by the game design team from the participant ideas that were analyzed in the final Capstone Event.[264]

The Capstone Event itself was a "one-sided, seminar-style, scenario-based game" with three operational teams, each assigned one of the C2 options, set within a fictional context of a Red team and regional neighbors in a series of four vignettes.[265] The three options were: domain commanders, cross-domain commanders, and functional commanders, with different separations of hierarchy and command based on domains or joint capabilities.[266] The fictional setting placed the teams as Blue against Red, with the goal of deterring red or defeating Red's anti-access and area-denial capabilities. Blue was warned that "Red would attempt to degrade Blue's use of electromagnetic spectrum, to include disruption of space and cyber systems, targeting both fielded forces and headquarters' C2 systems."[267] Participants had to decide how the four key functions, "deliberate and dynamic targeting," the intelligence cycle, "integrated air and missile defense, sustainment," played out within their command structure, and then were run through vignettes that helped evaluate 'what if' scenarios. In the end, they reviewed their assigned C2 systems according to six criteria: "unity of effort, flexibility, simplicity, resiliency, operational integration, and cross-domain synergy" and four processes: [268] After the initial review of their systems, players were able to alter the "command nodes and authority links" alongside the "role and responsibilities" of their systems, and present

[264] Marrin, Berberick, and Department, 1.
[265] Marrin, Berberick, and Department, 1.
[266] Marrin, Berberick, and Department, 3–5. The full command structures in diagram form are available in the game report.
[267] Marrin, Berberick, and Department, 28.
[268] Marrin, Berberick, and Department, 2.

their revised form for peer feedback, along with another round of revision and presentations.[269] The implementation of the game results was intended to "inform the development and refinement of a Joint XDO [Cross-Domain Operations] C2 [Command and Control] CONOPS," with a timeline of identifying and analyzing C2 structures in 2013 and then drafting and examining the CONOPS to support TTP (tactics, techniques, and procedures) in 2014.[270]

Global Title X Series '13 gameplay summary describes the cyber integration of the three systems, which is a structural description of roles and responsibilities.[271] The game report also lists a series of findings and recommendations on structure: "enhancing the unity of effort through mission command and authorities," the pace of structural changes and players preferring "evolutionary" shifts rather than "revolutionary" ones, the effect of "degraded communications environments," domain categorizations, and the control of the commanders.[272]

Game Analysis

Global Title' 13's purpose was to investigate future potential structures, and cyberspace operations played a role in affecting the utility of those options. The results of the game found that there was no overarching preference for one particular system over another, each had its strengths and weakness. While this does not perfectly answer the research question, it does explore the proposed control and command systems and models how they would function in a conflict.

---

[269] Marrin, Berberick, and Department, 2.
[270] Marrin, Berberick, and Department, 1.
[271] Marrin, Berberick, and Department, 35–49.
[272] Marrin, Berberick, and Department, 50–54.

The results section of the report is extensive, showing how players rated criteria, breaking down identification and mitigation of weaknesses, comparing the three approaches, as well as creating a plan for the next iteration of the game. However, there is notably little data regarding the actual design of the game. The report does not include a description of the vignettes or how cyberspace and conflict were abstracted; based on the findings, a reader could conclude that cyberspace was represented in a way that allowed for testing of intelligence, communication, and offensive cyber operations but without specificity as to the methodology. This would be helpful not only for verification of results but also for seeing whether or not the vignettes were realistic and based on scenarios that could be plausible or likely in the real world. The replicability of the game, based on the provided report, is very low.

The report follows a very similar style as the previous title, however, it does not include a limitations section, which the designers include in the next Title 14 series as a 'buyers beware' section. This is due to inconsistency with report writing and sponsor guidelines, rather than any particular inclusion or exclusion.[273] The report tracks the C2 Requirements Workshop's analysis and results, the C2 Options Workshop and an overview of the options, analysis, and results, and the Global Capstone Event. . Upon an interview with the designers, they mentioned that this is due to non-standardized report writing based on what the sponsor wants to know.[274] It is an ongoing debate within the community on how much information a report needs to have. Should there be enough information, for instance, for someone else to be able to replicate your game with your

[273] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[274] Marrin, Vogt, and Pellegrino.

report as an instructional guideline? Marrin, Vogt, and Pellegrino approach the reporting process as consideration for the function of the report as enough to understand the broad design considerations, the process, and the findings, but not to the extent that experiments must reach to be published.[275] The report structure does raise a point that wargame reports have no common framework in the same way that academic articles do. Even with the same designers, same sponsors, and same series, there are variations within the report and level of detail.

Global Title 14

Global Title 14 is a "1/5 sided, open intelligence C2 game and used an action-reaction format."[276] It was focused on the deliberation of tactical engagements in a command and control structure, not the outcome of those engagements. The previous game iteration's "Way Ahead" section states that: "Global 2013 will explore how the four emerging C2 attributes (information warfare/dominance commander, sustainment commander, cross-domain coordination and control element, and combined joint task units) derived from Global 2013 could be integrated into the current functional component model of today."[277] Global '14 has a workshop and a game component. The workshop refined four command and control attributes: "A Combined Joint Force Information Component Commander, A Combined Joint Force Sustainment Component Commander, Cross-Domain Operations Coordination Elements, and Combined Joint

[275] Marrin, Vogt, and Pellegrino.
[276] Don Marrin, Walter Berberick, and Wargaming Department, "Global Title X Series '14," Game Reports (U.S. Naval War College, 2015), 7, https://digital-commons.usnwc.edu/game-reports/15/.
[277] Marrin, Berberick, and Department, "Global Title X Series '13: Game Report," 57.

Task Units," these then formed a "Joint XDO C2 Concept of Operations."[278] The game has two objectives based on the workshop developments: "Identify any strengths and weaknesses of the four new C2 attributes (SCC, ICC, XDOCE, CJTU)" and "Identify improvements to the draft CONOPS and new Mission Essential Tasks."[279]

This led to three specific research questions:

"1. Based on the six C2 criteria employed in this game, how, if at all, does the integration of the four new C2 attributes (SCC, ICC, XDOCE, and CJTU) strengthen or weaken the ability to C2 combined forces conducting XDO in a high-intensity A2/AD environment? 2. What new authorities, processes, responsibilities, and mission essential tasks are required of the four new C2 attributes in order to plan, direct, monitor, and assess XDO in a high-intensity A2/AD environment? 3. In what ways does the integration of the four new C2 attributes impact current command and control authorities, processes, and responsibilities at the task force (Tier 2), component (Tier 3), and the task unit (Tier 4) levels of command?"[280]

The game is set in a fictional environment, named "Bartland," with no connection to real-world countries, with five countries in the region: Red – the hostile country, Green – the closest to Blue, and Brown, Gray, and Purple – with lower levels of support and industrialization. The Blue team, representing Australia, Canada, Great Britain, and Japan, was led by a USN O-8, and the Red team was led by the War Game Department's Office of Naval Intelligence Detachment, which also worked with the White/Control team. The game functions as an action, reaction dynamic with a four-hour turn cycle:

---

[278] Marrin, Berberick, and Department, "Global Title X Series '14," 1.
[279] Marrin, Berberick, and Department, 3.
[280] Marrin, Berberick, and Department, 4.

submission of an integrated task order, adjudication and forces movement, resolution of offensive and defensive actions, and the other team's turn consisting of the same movements. There were six turns in the week-long run, with an end-of-turn and end-of-day survey, as well as a final survey.

The teams primarily communicated via chat, and commands were sent through email – information degradation was a component of the game, affected by cyberspace operations, satellite functions, and jamming. There were domains of warfare: cyber, counter-space, anti-air, ballistic missiles, naval surface, undersea, and ground-based strike warfare.[281] Combat occurred on a map, and cyberspace operations affected kinetic systems. Players were given simplified 'kill-chains' that they would need to complete when developing their strategy and actions. Kill chains in the game were laid out in a diagram provided to players, where there were four categories of components: Sensor, C2, Shooter, and Missile, and counters to these components. [282] The components would also be connected through various channels, such as radio, land line, and missile flight. For instance, to deploy the antiship ballistic missile kill chain, platers would need to show that they had a sensor with a command and control ops center that lead to a shooter that connected to a target. [283] Along the way, each component of the kill chain could have counters both kinetic and cyber-related, such as jammers, dazzlers, or anti-satellite missiles. The LEO satellite was vulnerable to cyber-attacks, for example, but the Land Attack Cruise Missile system shooter had no counter. [284]

---

[281] Marrin, Berberick, and Department, 11.
[282] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[283] Marrin, Vogt, and Pellegrino.
[284] Marrin, Vogt, and Pellegrino.

The game found the strengths and weaknesses and recommendations for the four C2 attributes, which discusses the findings, discussions, and recommendations. The final findings were that certain command structures should be implemented, pursued, or require further evaluation. The limitations and game design analysis section notes that the game results are not generalizable, and lists the specific design limitations.[285] Because the command structures were built by control, players did not understand why the structures were designed that way. All the Tier 4, higher-level players, had perfect situational awareness because they were physically located with their fellow players, and they were overloaded with movement authority. Move forms were affected by limited time and degraded communications, which meant less data was collected as players cut short their communications. Internal validity relied on the quality and accuracy of data and data analysis (the player communications, final briefs, and surveys) while external validity was low, the game was not generalizable because the applicant pool was not reflective of all stakeholders.[286]

Game Analysis

Global ’14 had the same purpose as the previous game, but with greater refinement and focus on certain aspects of utility for C2 structures. The findings of the report correspond with the initial three research questions on the game design and include actionable material. The report is more extensive and in-depth than the previous year’s report and includes the limitations of design as well as a disclaimer regarding generalizability. Global ’14’s report includes information that there were cyberspace

[285] Marrin, Berberick, and Department, “Global Title X Series ’14,” 12.
[286] Marrin, Berberick, and Department, 13.

operations and a cyberattack kill chain, but the specifics were limited to further interviews with the designers of the report.[287] Global Title 14 includes a breakdown of demographics for the players, including their experience level and job, which is helpful for understanding whether or not the players are reflective of the real-world decision-making chain.

The representation of cyberspace operations in regards to their disablement and degrading capabilities was at a higher level of technicality; the representation of cyber broke down into tactical operations – choosing a specific component of a unit to degrade, but for a larger campaign in conflict. This may be more specific than strictly necessary, given that the purpose of the game is to test command and control structures, a similar result could have been achieved via probability rolls and observing the effect if a technology system goes down rather than having to explain how it went down – it does give officers that may not have cyber-specific experience the opportunity to think about defense and attack dynamics in cyberspace that effect kinetic structures.

Defend Forward Critical Infrastructure Game

In 2019, the Naval War College's Cyber and Innovation Policy Institute designed a cyber wargame, motivated by the 2018 Department of Defense's Cyber Strategy of "Defend Forward."[288] The Defend Forward: Critical Infrastructure Wargame was a

---

[287] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.

[288] Cyber and Innovation Policy Institute Staff, "Defend Forward: Critical Infrastructure War Game 2019 Game Report" (Cyber and Innovation Policy Institute, 2019), https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Cyber%20&%20Innovation%20Policy%20Institute/Defend%20Forward%20Critical%20Infrastructure%20Game%20Report%202019.pdf?sr=b&si=DNNFileManagerPolicy&sig=%2Bdh86X6w60GJ4B6iTHCbiq3T8iOQ8Oy0PIIlZiCbzUM%3D.

"three-move, move-step, free play game."[289] Over 100 participants of private sector business leaders, practitioners, and experts were broken into private sector leaders for Blue State companies (electric and finance) executives, practitioners in the Blue State government, subject matter experts (cyber, military, regional) into the Red State adversary, and subject matter experts for a White Cell that was meant to assess and adjudicate the player cells, facilitate the game dynamics (playing out the results of actions and updating the game situation), and act as the Green State, the ally of the Blue State, as well as non-state actors or the public[290] While the Blue State had no defined objectives or constraints other than player/cell interactions, the Red State specifically was asked to: Maintain international stability, regime survival, economic stability and growth, Green State influence, and Blue State intelligence gathering, while: avoiding direct armed conflict or directly provoke armed conflict and embarrassment of the Red State.[291] The scenario for the wargame was "economic competition between two peer competitor states, and in which Red State was conducting a cyber campaign to gain economic leverage and expose vulnerabilities for potential use in a future conflict."[292]

Within each move, players had five options: (1) Actions – issuing orders involving a specific "entity or component… what the action was, broadly how it would be accomplished, and why they were taking that action…and what they perceived the ideal and worst outcomes of the action to be." (2) Communication – sending 'emails' to other groups (but not individual players), (3) Press Releases – public official statements

[289] Cyber and Innovation Policy Institute Staff, 3.
[290] Cyber and Innovation Policy Institute Staff, 3.
[291] Cyber and Innovation Policy Institute Staff, 29.
[292] Cyber and Innovation Policy Institute Staff, 5.

to all players, which could also influence the 'public' played by the White Cell. (4) Chat Function – players in the Financial Sector Cell and DHS could communicate in the 'FS-ISAC' chatroom while players in the Electricity Subsector Cell and DHS were in "E-ISAC', or players could establish new chatrooms. (5) Request for Government Aid – private sector cells could request aid from the blue state government cell, requiring a specific support (cyber defense, cyber forensics, cyber mediation, counter cyber actions, emergency management, domestic policy creation, and foreign policy action), specific why, and the best and worst case of that action. (6) Respond to Request for Government Aid – Blue State Government players could respond to a request, but also could take a corresponding action if they so desired.[293] Data was collected via observation of the players' conversations and social dynamics, the GameNet chats, and surveys after each move asking about motivations for actions and views of the gameplay.

Gameplay began with pre-existing cyber campaigns, constantly according to "noise" campaigns (non-state actor attacks), some of which the White Cell had attribution for, and some of which had no confirmed attribution), and players were able to utilize "counter-cyber" capabilities.

The specific cyber capabilities for each state are as follows in the report:

Blue State, under the Military brief:[294]

- Cyber capabilities
    - Highly developed offensive capabilities

[293] Cyber and Innovation Policy Institute Staff, 32–34.
[294] Cyber and Innovation Policy Institute Staff, "Defend Forward: Critical Infrastructure War Game 2019 Game Report."

    - Cyber Defensive Teams
- Blue State Cyber Capabilities managed by: DHS, DOE, DOT, DOD, DOJ/FBI

Blue State Government Cell Briefing:

- Knowledge of Red-State offensive and defensive capabilities:
    - "Can be utilized in conjunction with or independently of military operations
    - Integrated into military operations
- Integrated defensive cyber capability
    - Cyber defensive operations are routine
    - Integrated into military operations
    - Protection of certain civilian networks

Blue State Cyber Campaigns Against Red State:

- Espionage against Red State Foreign ministry networks and Red State Office of the President
- Espionage, degradation, or disruption against Red State Military Logistics Agency and Red State Navy
- Degradation, disruption, or destruction against Red State critical infrastructure
- Espionage, degradation, or destruction against Red State Intelligence Services, Cyber Operations Command

Red State, under the Military section:[295]

- "Cyber Capabilities:

[295] Cyber and Innovation Policy Institute Staff.

    - Large focus on cyber capabilities in the military, special forces, and intelligence
    - Primarily uses cyber operations in peacetime for:
        - Pre-staging access/exploits for later use in crisis
        - Generational situational awareness intelligence
        - Intellectual-property theft
    - For game purposes, assume both offensive and defensive cyber capabilities
        - Known successes with infiltrating supply chains, unconventional accesses, and large scale data breaches
- Does not typically use cyber-enabled information operations"[296]

Red State Cyber Campaigns:

- Espionage against Blue State DOD/OSD unclassified networks, OPM Databases, Blue State Office of the Trade Representative networks, Blue State business operations of electric companies, Blue State financial services, Green State op Espionage, degradation, or disruption against position leadership, and Green State Ministry of Defense
- Espionage, degradation, or disruption against Executive Office of the President unclassified networks, GRAYCOM classified networks
- Supply chain attack or espionage against Blue System Engineering classified networks

[296] Cyber and Innovation Policy Institute Staff, 16.

- Degradation, disruption, or destruction of Blue State electrical utilities

The Green State has no cyber capabilities listed, and non-state actors had 'noisy' cyber attacks, such as data theft, denial of service, malware, ransomware, etc.[297]

While the goal of the game was to analyze Defend Forward, given the uncertainty surrounding its strategy and implementations, the analysis of the game created a "small number of findings" that are "suggestive, not definitive."[298] The game found that: the Blue State (a) attempted to create "mutual vulnerabilities within critical infrastructure and then [conduct] offensive operations on these infrastructures in both allied and adversary nations to deter further escalation," (b) aided in defensive capabilities of the Green State, (c) utilized counter-cyber operations, and (d) highlighted private sector and government clash as the former worried about "negative implications for consumer confidence and global markets."[299]

Game Analysis

The first thing of note is that, if the goal of the wargame was "Defending Forward: Wargaming a Cyber Strategy," then the Blue State should have been explicitly provided with the Defend Forward 2018 strategy as an objective, in the same way, that the Red State was provided with objectives. While abstraction is a valid method for attempting to negate pre-conceived player notions of one state or another, the Blue and Red State functions and objectives allow for relatively simple abstraction to US and China given the set-up of the Blue and Red State functions and the Red State objectives.

[297] Cyber and Innovation Policy Institute Staff, 6.
[298] Cyber and Innovation Policy Institute Staff, 8.
[299] Cyber and Innovation Policy Institute Staff, 8.

That's not to say that valuable information was not gained from the wargame, however, given the set-up of the game itself, the test appears to be less on "[examining] the implications of different conceptualizations of Defend Forward, operational implementation, as well as their domestic impacts" and more "how do private and public sectors react and interact when faced with cyber campaigns conducted by an adversarial state?" While the participants in the Blue State government and Red State government were experts and practitioners that very likely were familiar with the Defend Forward strategy, releasing it as required reading for all participants including private sector role-players would have given greater direction to the game itself and actions taken within that game.

The cyberspace operations in the wargame were "highly abstract and non-technical, derived entirely from unclassified, open-source research."[300] As evidenced from the listing of the cyber capabilities, there were very few 'explicit' guidelines regarding cyber operations. This offers both positives and negatives: the first being that the game can be unclassified, reaching a broader audience, the second being the cyber operations requested are only limited by the imaginations of the players without too much required technical knowledge: "We are using X capability to do Y for Z reasons."[301] However, while players were deliberately chosen as experts, the high-level abstraction of cyber operations, alongside a lack of methodology or information on White Cell adjudication, could have created a false tit-for-tat narrative that led to the concerns regarding escalation. Secondly, a lack of White Cell methodology or analysis makes

[300] Cyber and Innovation Policy Institute Staff, 28.
[301] Cyber and Innovation Policy Institute Staff, 32.

analyzing the 'realism' of the game difficult. For instance, cyber operations intended to degrade or destroy infrastructure capabilities state that substantial downtime may be required, while the wargame itself was meant to represent 180 days (Move 1), 30 days (Move 2), and 30 days (Move 3) for a total of roughly eight months. Was the success of large-scale infrastructure attacks adjudicated based on the known-planning time of similar attacks? This wargame deliberately removed the technical concerns, but in doing so, it created a potentially accelerated or slowed action-response-reaction timeline that also could have increased player escalation concerns. As noted in the previous section, the utilization of cyber as a 'tool' for deterrence, denial, and punishment is difficult because of attribution and timeframe. However, the inclusion of "noise" attacks from the White Cell was a way to address the issue of a too-clear tit-for-tat communication between the Red and Blue State.

Of note in the findings sections, "players indicated that they had no clear way to request or advocate for counter-cyber operations that would degrade adversary capabilities to conduct cyber operations against their infrastructure."[302]This influences and limits the *action set* players felt they have access to. For instance, the outcome of the game could have been far less aggressive, resulting in less private-sector concern, if clear defensive and degradation of adversary offensive capabilities, as opposed to mutual vulnerability attacks, were listed. The presentation of the options set could have influenced the Blue State in Move 1 utilizing offensive cyber operations in response to Red State cyber operations, resulting in a final "significant increase in tensions and

[302] Cyber and Innovation Policy Institute Staff, 8.

hostilities between the Blue State and Red State" by Move 3.[303] The authors of the study recognize this, noting that while players supported counter-cyber operations, they were concerned that the "mutual vulnerability strategy of attacking critical infrastructure" could result in harmful escalation. [304]

Educational

Merlin[305]

Merlin is a wargaming module, sponsored by the Air Force and designed by the Center for Naval Analyses. There are two versions of the game, one designed for a large wargame audience with detailed mechanics and adjudication, and another 'off-the-shelf' stripped-down version.

The game is intended to help players "think creatively about cyber tradecraft, understand what goes into it in terms of the time it takes to create and deploy it, and the personnel and organizations the creation entails. It's about thinking creatively and getting operators from air, sea, and land, to talk to cyber operators in terms that all can understand – to put cyber on the same level in the operational terrain. But, it also forces players to understand that cyber is a limited resource and forces them to make choices about what sort of cyber tradecraft they want or need."[306]

The larger-scale version was created because of a concern that there was a lack of cyber representation in Title 10 service-sponsored wargames, which are detailed, large-

[303] Cyber and Innovation Policy Institute Staff, 7.
[304] Cyber and Innovation Policy Institute Staff, 8.
[305] The description of the game is based on an interview with one of the CNA designers, and this section is paraphrased from the interview. Some aspects of the game are not addressed for security reasons. Lea, Interview with Kate Lea.
[306] Lea.

scale games that the services run every year. Merlin was developed for cyber integration into these games. The target audience for the off-the-shelf version is a lower-level command that would use the game for training and education to help their personnel how cyberspace campaigns could impact them and vice versa. The game development has been several years in the process.

The main difference between the 'off-the-shelf' version and the full version is that the former is intended to be run without an adjudicator. While first-time demonstrations involve an adjudicator from CNA, players can pick up the game after the initial run-through to be able to play without a games master.

One scenario of the off-the-shelf version is based on a fictitious alternative history set in North Africa, with countries that do not exist, showcasing a notional conflict over resources. Players have a stripped-down order of battle, with limited military assets and three possible action types. They can either conduct peace-time troop movements – posture forces, a kinetic operation – fight, or a cyber operation. Each of these operations has a different time scale. Peace-time troop movements take weeks to move forces, kinetic operations take place within hours, and cyber operations can occur within mere minutes. However, cyber operations also have a developmental timeline, and therefore players must roll a dice to determine how long the cyber operation took to plan and create before game time.

In the off-the-shelf version of the game, players get a certain amount of resources that they can expend, but time is a resource, and therefore as they create their tradecraft, they eventually plan further and further back in time until they reach the end of their

timeline. So, eventually, there are tradecrafts created that can't be used for several turns, which shows players the resource constraints inherent in cyber operations.

The cyber tradecraft is up to player creativity. The game abstracts the targets and accesses into several categories, and so players need to determine what type of target they are trying to affect out of five choices, and what access approach they are using from three options. Each choice influences the dice roll on the time scale investment. For instance, if players want to access a weapons system, this is a 'larger' dice roll (i.e., requiring more time to access) because weapons systems are often not connected to the internet and these systems tend to be more secure. Players also must address the effects of their cyber tradecraft: the intended effect and outcome; in other words what it is intended to do and why that matters for the game.

After creating and deploying their cyber tradecraft, players have success and burn roles. The baseline chances for success and burn are 80% and 20% respectively, but players can negotiate with each other and with the adjudicator to alter their chances based on arguing for the effectiveness of their capabilities versus the potential for an adversary to burn it. An interesting note is that, for the off-the-shelf version, players do take advantage of the success and burn alterations, but over time, they tend to default to the base probabilities.

Impact Observations

In the unclassified scenario of the off-the-shelf version of Merlin, players have not tended to be cyber operators and therefore have limited cyber expertise. It is a learning experience for them to become more comfortable with creating cyber tradecraft and calculating how different access approaches to different target types will change the consumption of cyber resources.

In the full version of Merlin, cyber operators gain a better understanding of what terrestrial operators want out of their cyber tradecraft, and terrestrial operations become more versed in what cyber can do. The off-the-shelf game is more popular among cyber operators, who use it as a training module and for professional development.

Given that the purpose of Merlin is to act as a communication tool and discussion between cyber experts and cyber operators, the format of the module serves its intent, to the best understanding that a description of the game can offer. Merlin also offers the added flexibility of being a module, or a tool, that can be slotted into other games without cyber elements. This grants it more utility than some of the larger-scale bespoke games utilized by the services, and the ability to switch out scenarios based on use cases makes the game easily adaptable to current-day issues.

Women in Command: Hybrid Threat Rising

Women in Command: Hybrid Threat Rising is an "educational two-team game aimed at introducing women to wargaming and international conflict resolution" as Turkey's first hybrid civil warfare game.[307] The game is based on real-world events and research, simulating the conflict in 2014 between Russia and Ukraine.[308]

The setting of the game places Astraidor, a fictional red state, against Vercrania, a fictional blue state. Each has different win conditions. Astraidor's ideal end goal is to secure the regions of Oplin, Azmarin, Vizalis, and Kaldair, block international and NATO involvement, capture other regions and use hybrid operations to deteriorate the government and society of Vercrania. Vercrania needs to recapture Oplin without losing

[307] SAYIN, Interview with Elçin Ada SAYIN; KızBaşına Women in Command Project Team, "Hybrid Threat Rising Wargame" (KizBasina, 2021).
[308] SAYIN, Interview with Elçin Ada SAYIN.

moral superiority, block military presence in Vizalis, Azmarin, and Kaldair, and block further Astraidor influence.

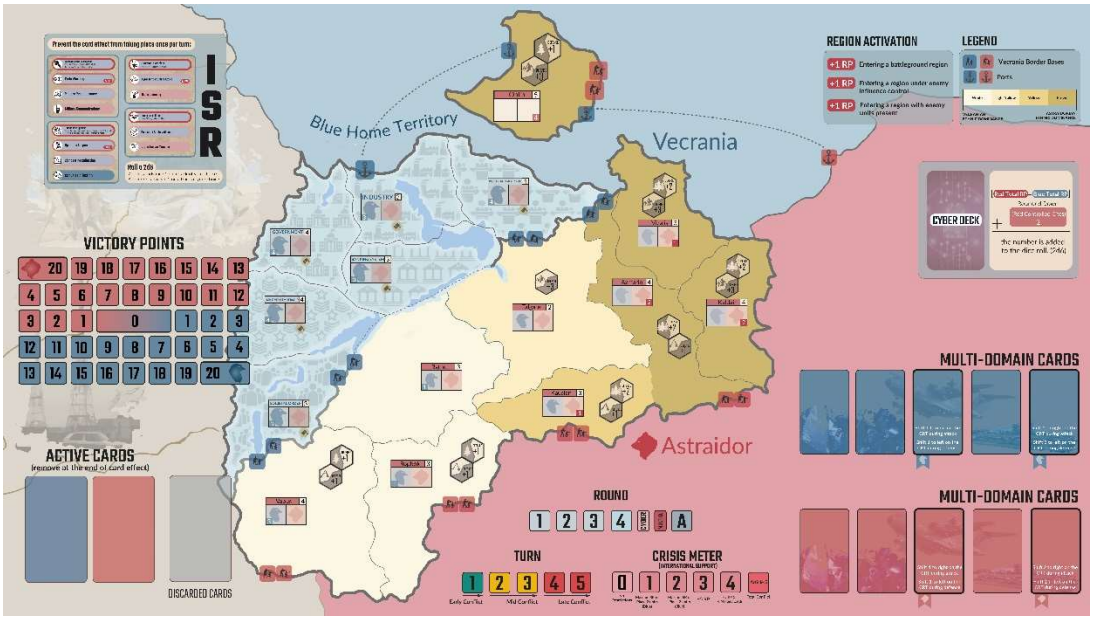

Figure 2. Map of Hybrid Rising Threats (KızBaşına Women in Command Project Team, "Hybrid Threat Rising Wargame" (KizBasina, 2021).)

The game operates with a victory point system, where the first country to reach 20 victory points wins, or at the end of two hours, the team with the highest points wins. There is also a crisis meter which, if triggered to total conflict, becomes an automatic victory for the Blue because there will be international support under Article 5. The game is a simulation of hybrid warfare, with military cards: multi-domain, operation, and mobilization, cyber cards, unit tokens representing military units, influence tokens, and resource tokens. There are three stages to the game: early, mid, and late conflict with five turns. Each stage has different capabilities in regards to its event cards, and the turns follow with four event rounds, then a cyber attack, a multi-domain operation, and an

action (involving on the ground forces) round. During the action round, players play operation cards, activate to move and initiate combat, and mobilize and prepare. During each turn, each team takes turns playing their event cards, triggering their effects, or investing the card into ISR capabilities. The ISR effects impact resource investment and combat. The game guide notes, specific to cyberspace operations, that early Intelligence, Surveillance, Reconnaissance, and multi-domain control are critical to Astraidor.

There are seven offensive cyber capabilities, each with a low, middle, or high effect depending on the roll that result in Vercranian loss of resource points or influence, ISR regression, or unit withdrawal or removal within a region or from battle

- Attack on Military Personnel: social media phishing accounts targeting Vercrania military personnel that send malware files for sensitive credentials
- Power Outage: Cyber attack resulting in a power outage on Vercrania
- Train Accident: Train crash near Talgate as a result of a cyber attack
- Water Supply Delivery: Drinking water supply chain is attacked
- Target on Artillery: Astoraidorian malware destroys the majority of Vercranian rocket forces and artillery
- Vecranian Postal Service: CryBaby ransomware disables the transportation company for critical military equipment and the postal service
- Email Leak: An Anti-Astraidorian politician has his emails leaked and spread

Only Astradior has offensive cyber capabilities, Vercrania only has one card for defense, three copies of a Cyber Intelligence card: Vecrania gains intel on an Astraidor

attack and takes precautions, blocks a cyber roll for the turn. If this is drawn during a turn, then Red cannot attack.

For a cyber attack to initiate, Red plays the card and then rolls a 2d6 to add to an equation of Red total Resource Points – Blue total resource points + Red Controlled Cities/2 (rounded down). A low effect is a 7-8, the middle is 8-10, and a high effect is 11-12.

Game Analysis

Hybrid Threat Rising attempts to model multi-domain hybrid conflict, which can be difficult because of how all-encompassing it is. The game itself is based on real-world research and pulls its cyber attack and multi-domain scenarios from the NATO Cyber Security Excellence Center International Locked Shields Cyber Exercise.[309] It abstracts out cyber events into attacks on critical infrastructure or politics on an overarching strategic level. Although the events are limited to cyber-attacks that mainly irritate through resource or influence loss, with only higher-level rolls affecting military combat, this is reflective of expert opinion that cyber is not a decisive element in military combat, nor was it in the Russian-Ukrainian conflict.[310] Cyber attacks also do not require a resource cost to play, but Hybrid Threat Rising does create a unique formula that attempts to take into account the overall power of the Red versus Blue country as a proxy for cyber success probability.

Given that this game is intended as entry-level, keeping the card decks to a smaller size is conducive to gameplay, particularly because there are so many domains and events to handle. In an initial run-through of the game, sponsored by the Georgetown

[309] SAYIN.
[310] SAYIN.

Wargaming Society, the game took a couple of turns to fully pick up, and even after players understood how it worked, it still took over two hours of game time to become comfortable, let alone think strategically about how to win the game.[311] Cyber attacks were viewed more as an irritant than strategically decisive, but technology investment into ISR was heavily leaned upon, especially in earlier rounds.[312] The game is not highly realistic because it is limited, but that is where its value is derived, because it creates an understandable way for non-defense or military experts to understand how multi-domain combat fits together. For a non-public audience, the utility is likely lower, but the game could emphasize for decision-makers how seemingly detached civilian infrastructure events, like a postal service hack, could disrupt military objectives. It also illustrates cyber imbalances within country-to-country conflict. Other games have given cyber capabilities to red and blue players that are slightly in favor of one or the other, but this game reflects Haggman's Cyber Security Game, where one side has a massive offensive advantage and the other side can do little but defend.

Cyber Card Game[313]

"The Dstl Cyber Red Team Game was developed as a research innovation by-product during Dstl Cyber Resilience Advice to UK Critical National Infrastructure & Military Platforms. The rationale is that those defending Cyber-Enabled Critical National Infrastructure (CNI) or military enterprise systems will benefit from learning to think like

[311] KızBaşına Women in Command Project Team, GUWS x KizBasina: Hybrid Threats Rising Playthrough, February 19, 2022.
[312] KızBaşına Women in Command Project Team.
[313] I was able to play this game through a Georgetown Wargaming Society sponsored session. While I am currently requesting permission from the Dtsl's Intellectual Property form, the format and the capabilities of the game are based on in-game collected notes.

an attacker. By playing the attacker within an unclassified scenario environment, the defender can better understand the actions required to increase cyber resilience."[314]

The Cyber Card Game is a cooperative, one-sided, small-team game that pits players as the offensive cyber team of Redland against a hypothetical Blueland. There is a third party, Yellowland. Yellowland has weak Blue-land leadership and pro-Redland rebels; Blueland is offering a peace-keeping force to Yellowland to prevent the rebel growth. The majority of Yellowland does not have a strong political swing – their main concern is stability.

The port has several key sites, including locations for fuel storage and transfer, buildings and warehouses with unknown utility, a fuel transfer, and fuel storage site, a rail yard, a vehicle park, and a server building. It also has several entrances, a road entrance, a rail entrance, a perimeter fence, cranes, containers, and a lock for the port. The red team intelligence briefing notes that the port is where the Blueland has the majority of its fleet, is responsible for military fuel, and is critical to the Blueland operations and defense force.

The red team is given some explicit orders: Target the Blueland Military port. Discredit, degrade, delay, disrupt, or deny blue access to port ability to deploy support to Yellowland. There are no limits on collateral damage and no targets are under no-strike orders. Any damage done should ideally be non-attributable, and the
They receive 24 resource tokens for the entire game, which represent a broad category of resources such as time, money, manpower, etc. needed to conduct the operation. The

[314] Dstl, "Cyber Card Game" (Dstl, n.d.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043232/Easy_Access_IP_Cyber_Card_Game.pdf.

timeline of the game is approximately two weeks, but the goal is to be accomplished as soon as possible.

Player Experience[315]

I had the opportunity to play this game, run by Tom Mouat, and sponsored by the Georgetown Wargaming Society, therefore, this game will only address the capabilities and gameplay options that I was able to observe. There are other branching options depending on what cyber tools and methods are used according to team choice, but this will only address the decision-making in one instance of the game.

The game begins with deciding what reconnaissance to conduct. There are seven options with varying costs: the team can choose whether to conduct a physical survey, an open-source survey, exploit social media, probe search engines, use an external network probe, an internal network scan, or a network traffic survey. Some of these options require an established network presence, which the team did not have.

After discussion, the team went with an external network probe and discovered information regarding the vulnerability of the router, email server, login credentials, and what filters existed on the network.

Next, the team needed to decide how to gain access via another seven options: spear phishing, wifi-pivot, exploit ICS links, media data inject, watering hole, router hack, and insider. Each of these had certain information requirements, such as knowing an email address to spear phish or knowledge of internet patterns for a watering hole attack. These options also had low-cost and high-cost investments options of resources, which altered the rate of success. If a roll failed at a low cost, the team could pay the

[315] Mouat, "Cyber Card Game."

higher cost to try again with better odds. However, rolling too successfully would result in a possible detection because the intrusion would be too successful. The team chose to conduct a router hack, given that we already had the required information on the router from the external probe, which gave players access to six systems: the port HQ, the fuel process control system, the logistics database, the power and lock management, the warehouse management system, and the dockyard wireless system.

The last step was to choose and plan the attack. Attack options also had low and high-cost values, and this was where the majority of resources were spent. There were nine options: trashing the domain, denial of service, website defacement, jamming wi-fi, user interface manipulation, over-ride sensor feed, database injection, control of the ICS through credentials, and process logic controller factory reset. The team decided to over-ride sensor feed, which failed, and then players paid to succeed. Next, we conducted an ICS UI attack to flood the port with oil using the fuel control system, and then tried to do a PLC factory reset to cover our tracks. These succeeded, and the team also succeeded in the attribution check, meaning Red accomplished their goal of disabling the port with deniability.

Game Analysis

The technical representation of cyber in this game was more realistic because it was a tactical game, where individual steps in the cyber kill chain were laid out with detailed technical terms and required links between them. For instance, there were attack options and access options not available to the team because we did not invest resources into establishing the ground information or intrusion requirements. The game itself is also built for a very fast pick-up and gameplay, taking around two hours. Players did not have

to read a rule book or sit through an explanation of mechanics, instead, they were quickly thrown into the game, and mechanics such as the low-cost high-cost or kill chain steps were introduced along the way.

The fictional setting of the game grants it flexibility; Mouat noted that the Cyber Card Game was not intended to represent one scenario or another. However, although the game is educational, it can also very easily have an analytical real-world setting that investigates the different attack paths for accessing a port. When planning the time of attack based on the routes of ships and port open/closures, players were directed to the live camera and port monitoring of a real-world port.

The level of technical detail in the game is at the point where non-cyber-experts can be educated on the cyber kill-chain while contributing to the discussion based on common-sense and creative thinking, for instance, a player was able to suggest ransomware and blackmail as a possible chained intrusion method. However, the level of technical detail during the discussion proved incomprehensible for some players, given that about half the team did have a more technical background or more experience with cyber security. This occurred mainly during the attack phase discussion and led to players eventually running out of time to make a decision and having to rush to carry out their final attack. This is not necessarily something that can be fixed with game design because the intrusion and access methods have descriptions on the card capabilities. Any further description, other than explaining how this action would affect the network of the system, would take away from the creative ‘thinking like an attacker’ aspect, where players are supposed to link together the tools to the ideal disablement together.

This is where, with a greater budget or more resource investment, a cyber expert 'on-call' could be beneficial which can explain further the potential impact of each cyber attack within the context of the port system. Given that the game was run with a single adjudicator, the adjudicator could not give suggestions as to attack opportunities because it would disturb the learning and flow of the game.

During the 'hot wash' or the discussion after the game, Mouat mentioned that the game was designed with a deliberate element missing: presence maintenance.[316] Typically, during a cyber intrusion, the goal would be to maintain access to the network rather than crash and burn the system after attempting to attack the port. Additionally, during the approximately two-week timeline, there would likely be regularly conducted tests to kick intruders out of the system. These were not represented within the game and could add another layer of complexity and realism because the game is one-sided, without any entity representing the defender team, and even the adjudicator represents the 'environment' of success and failure rather than the adversary.

This game addresses the understanding of cyber methods and rooting them in the context of potential impact, as well as understanding the vulnerabilities of critical infrastructure like ports. An interesting application in the future using the game as a base design could be seeing the different methods that players use to disable or degrade port capabilities, to prepare for various potential 'worst-case' scenarios. While the players in this playthrough chose a method without immediate causalities, spilling oil into the surrounding water systems, there still was a secondary environmental impact. Other observed plans conducted by other players did not minimize damage, such as shutting the

[316] Dstl, "Cyber Card Game."

gates when a ship was opening or closing, causing human causalities. Because this game combines technical methods with effects-based impact but uses generic technical access and reconnaissance methods, it does not cross any classified lines, nor does it become too technical.

Littoral Commander

Littoral Commander is a tactical wargame intended as a "custom-based learning and education game for company and enlisted officers to run for their NCOs (non-commissioned officers) and junior marines to explore how future warfare may look like in the 2030-2040 timeline." It allows players to "kick the tires conceptually at concepts that are transforming warfare" and see how it affects them at their level of command.[317] The game allows for 2-10 players, and plays with imperfect knowledge and covert planning, placing the United States against China in a variety of scenarios and maps that range from objectives like 'destroy all units,' 'deny passage,' 'reach a certain location,' or 'maintain force power in a certain area'. The gameplay incorporates physical units on a hex map, represented by unit tokens, and cyber and military operations via a card deck. Units can take a certain amount of hits, store ammo, and defend or attack. Gameplay is addressed in a turn cycle, and one turn represents about 2 hours of real-time. There are four stages: Planning – where card capabilities can be bought with command points, Deployment – setting units on the board, Action – where each player on a team, controlling a set of units, can either move and/or initiate combat, move and/or conceal, move and/or conduct resupply, or play a Joint Capability Card, and then an Initiative and

[317] Bae, Interview with Sebastian Bae.

Victory check to resolve the actions of the game into the gameplay mechanics of which team goes first and objective success.

Both sides start with their 'C5ISR' network that represents the core network of their country; for China, it is an advanced battlefield AI and for the U.S., it is an Advanced Battle Management System. When a successful cyber campaign is launched, players add a cube to the card, which can affect other roll probabilities the more successful campaigns are launched. The game rules note that "the wargame is unclassified, but only for education and training usage," and "users should not post detailed accounts of game moves….[which] limits the risk of the wargame being taken out of context."[318] Therefore, the game will list, in general terms, examples of cyber capabilities rather than a specific list.[319] The cyber cards are played as Joint Capability Cards, which can affect unit capabilities or respond to other cards, generally via a dice roll. For instance, there are EMP technology and anti-EMP shielding, different types of hacking or exploits, communication degradation, influence campaigns, general cyber or EMS defense, jamming, and network resilience. Rolls for combat or card success are

Game Analysis

Littoral Commander is a game that anyone with no experience can pick up, but it does have a learning curve. Upon two plays of the game, a player can expect to be relatively familiar with the structure, but, similar to other entertainment games like Twilight Struggle, strategic gameplay comes from familiarity with the capability set. This

[318] The full version of the game is available for purchase at the Dietz Foundation or on Table Top Simulator for a full list of capabilities. Sebastian Bae, "Littoral Commander" (Dietz Foundation, 2022).
[319] Bae.

can prove difficult given a card deck that is too large to be picked up on the first game playthrough, but this adds to the replay-ability factor.

Littoral Commander also comes with a variety of maps and scenarios based on hypothetical projections of future warfare. This grants it a high level of flexibility, because it can, and is, being updated as new technology is unclassified or speculated upon, or as new conflicts of interest arise.[320] The game is built at an entirely unclassified level, despite having designers with higher classification levels. During the design process, the team kept very close attention to their sources for the technology and assumptions built into the game and was able to utilize their running list of sources during the classification review for release.[321] Because the format of the game allows for easy adjustment of card capabilities and scenarios, the game can be updated to a classified level if more detail is needed or keep up with new developments.

The cyber element of the game models an excellent example of forcing players to make sure their cyber operations are directly connected to their battlefield decisions. Some cyber capabilities need to be attached to units, or some directly affect the battlefield power or ISR level. It also allows for creative gameplay and a strategy-based use of cyber, where some cyber capabilities will be launched only in conjunction with another attack or thrown out as a distraction. While the actual cyber action once played is overt, the purchasing of the capabilities is covert, allowing for the psychological element of uncertainty regarding an opponent's cyber capability.

[320] Bae, Interview with Sebastian Bae.
[321] Bae.

Cyber Security Strategy Game

The Cyber Security Strategy Game was prompted by the UK National Cyber Security Strategy, released in 2016.[322] The game is designed by Andrew Haggman as part of his Ph.D. thesis at Royal Holland University, and the goal of the game is education on cybersecurity and action-reaction.

The game rules can fit on a double A4 page, which takes players less than ten minutes to understand.[323] Set with real countries, the context puts Russia against the United Kingdom, Russia is represented by five actors: Government, Online Trolls, Energetic, Bear, Special Communications Service (SCS), and Rosenergoatom, while the UK is represented by: Government, Electorate, UK Plc (business), GCHQ (military and intelligence), and UK Energy.[324] The win condition is to collect more victory points, collectively on one side, which can be earned through attacks – a successful attack that drops another actor to zero or lower scores 10 victory points (VP) and ends the game, or through achieving win conditions, specific to each actor.

Each entity has different goals and ways to gain victory points:[325] The UK government's goals are to ensure popular support during the election by supporting the electorate and ending with anti-Russian rhetoric: +1 victory point for each month the electorate has 4+ resources and +5 victory points if the Russia government has less Vitality than it started with at the end of the game. The UK Electorate's goal is to maintain wealth: -1 victory point every time a resource is moved from its possession. The

[322] Haggman, Interview with Andrew Haggman.
[323] Haggman, "Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education," 92.
[324] Haggman, 295.
[325] Haggman, 207–20.

UK Plc's goal is to increase wealth in preparation for Brexit: +2 Victory Points for ending April with 3+ resources, +3 Victory Points for ending August with 6+ Resources, and +4 Victory Points for ending December with 9+ Resources. The GCHQ is trying to grow its human resources, and therefore if it increases vitality in each quarter, it gains Victory Points (+1 for one quarter, +3 for two consecutive quarters, +5 for three consecutive quarters, and +7 for the full year). UK Energy is trying to grow its energy output for the Electorate, and therefore it will +2 Victory Points for 6+ Vitality by June and +3 Victory Points for +9 Vitality by December.

The Russian government's goal is to retain wealth and regulate online trolls: +1 victory point for ending each month with 3+ resources, -1 victory point for an online troll 3 or 4 resource attack, and -2 victory points for a 5 or 6 attack. Online trolls have an objective opposing the government, launching large-scale attacks: +4 victory points for every 3+ resource attack with the ransomware asset. Energetic bear gains victory points for having more vitality than the start, April, August, and December at certain points in the game. The SCS wants to increase its cyber arms race, so it gains victory points by having more attack assets than the UK's defense assets. Lastly, the Rosenergoatom's goal is to increase the energy output, the same as the UK's energy group.

Gameplay switches between the two groups, with all actors completing their actions before moving on in 3 minutes. Actors within a side are connected in a certain pattern, representing their relationship, and actors on opposite sides are connected via attack vectors. During each turn, there are five available options using two resources, resource and vitality: distribute – move resources to another actor (maximum of five), revitalize – trade in resources for vitality (1 for 1, 2 for 2, 3 for 4, 4 for 5, 5 for 6, or 6 for

7), attack – use resources to attack (minimum cost of 1, maximum cost of 6), and abstain. GCHQ and SCS can access the black market to bid with resources – with all bids using resources regardless of whether or not the item is won.

Attacks are based on a Combat Resolution Table where scores are based on the damage to vitality of the attacked or self-damage for the specific actor. Damage will also ricochet to actors that are connected on a 1:2 ratio (both for successful and self-damage). Failed attacks are attributed, with two levels of attribution that result in a system modifier gain for the other team.

The Black Market opens up the cyber gameplay by introducing modifiers, there are nine: three offensive and six defensive.[326] There is an attack vector that introduces a new attack opportunity: GCHQ-Rosenergoatom, SCS-UK Energy, UK Gov-Russia Gov, Stuxnet 2.0 which doubles the damage of GCHQ-UK Energy or SCS to Rosenergoatom, and Ransomware which stuns the UK Plc or Electorate for 2 turns (or unstuns them for a cost of 2 resources for the attacker). The six defense assets include education, recovery management, software update, bargaining chip, network policy, and cyber investment program. These reduce damage or recover vitality. This market is shared, and teams must expend resources to gain upgrades. There are also 16 event card modifiers that change the vitality, resource allotment, or ability to bid on a certain entity. Eight cards have an effect: Nuclear Meltdown, Clumsy Civil Servant, Software Update, Banking Error, Embargoed, Lax OpSec, People's Revolt, and Quantum Breakthrough. The other eight cards are uneventful months where there is no modifier. This represents random occurrences in different domains that impact cyberspace operations.

[326] Haggman, 122.

Game Analysis

The game introduces several concepts useful for cyberspace operations: the entities of concern, varying 'win conditions' for different entities, and attack versus defense trade-offs. The Russian-UK conflict covers various entities, each with its own goals and success conditions, which helps players understand trade-offs between cyber operations; some victory point gains directly contradict the goals of other entities even on the same side.

The attack-defense cycle is represented in conflict and a purchase and upgrade style, and while the Black Market system is non-realistic, the purpose for introducing it was to attempt to represent a cyber arms race.[327] A more accurate representation of the game that may impart better knowledge would be if each country had its research and development resource investment turn, rather than operating on a shared bidding market, which is the weakest element of the game.[328] The level of technical detail represented in the game is low, it is heavily abstracted from reality, such as by limiting attack vectors or only having one generic base form of attack. However, it is a representation of resource investment and attack-defense considerations. Player feedback was focused on takeaways regarding the attack-defense cycle: the threat of another entity attacking (which, in the game, because a question of if, not when), and the strength of defense investments.[329]

The importance of *what* the game is imparting here is important and represents the danger of educational games being viewed as analytical or representative of real-

[327] Haggman, Interview with Andrew Haggman.
[328] Haggman.
[329] Haggman, "Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education," 196.

world conditions. For instance, Haggman found that a UK offensive strategy was very rarely successful, but, because the game is designed as an educational game – this may be indicative of game design rather than of any generalizable conclusion.[330] Additionally, while most players recognized the allure of attacking was due to game design, some players came away with frustration in regards to the lack of offensive capabilities for the UK.[331] This is where adjudication and an ending discussion are crucial because once players feel frustrated at game mechanics rather than at the other team, learning ability goes down.

Enterprise Defender

Enterprise Defender is a two-sided, educational game that models information warfare, specifically for non-IT managers or non-experts. Curry and Price list the educational goals as increasing knowledge of "potential threats" and "vulnerabilities", "range and purpose of existing IT security-related policies," and creating "an action plan for managers to take back to their team."[332] The game set-up has a hypothetical (or real-world if played by team members representing an actual business) set-up of defending the cyber systems and information of a business.

There are two sides: a 'hacker' team(s) that represents a rival business, and a 'cyber defense team' of the attacked business. There is also a control moderator that is a subject matter expert in IT and network defense.

[330] Haggman, 183.
[331] Haggman, 197–98.
[332] John Curry and Tim Price, *Dark Guest Training Games for Cyber Warfare*, 2013, 35.

The game progresses in three stages: Planning, Assault, and Hot Wash-Up.[333] During Planning, the defense team tries to come all with all the potential information warfare threat vulnerabilities and then create a list of defenses within three categories: physical, procedural, and ICT. Hackers create give attack methods and outcomes, written on cards. During Assault, the hacker team presents each attack, and then the defense must demonstrate how they could have detected the attack and then use their pre-brainstormed defenses to block the attack. Then, the umpire decides the chance of an attack succeeding based on how convincing the defense was, and a pair of six-sided dice are rolled to determine the success of the attack. Lastly, the hot wash is a discussion after the exercise about putting the potential attacks and defenses lessons into action.

Game Analysis

Enterprise Defender serves the purpose of testing the understanding and effectiveness of existing policies and improving the knowledge of players, which it accomplishes well given its very focused, minimalistic design. This game is the barebones of a 'wargame' but still technically meets the qualifications because it involves adversarial gameplay, players, decisions, and consequences. This makes it easy and quick to run by anyone with adjudication qualifications for anyone else, and it can be considered an easy entry method for using wargaming. The game's fidelity and utility, accomplishing its intended purpose of education, relies heavily on the participants' and the adjudicators' knowledge and imagination. This game does not present a list of cyber capabilities, instead, it relies on participants to come up with their attack and defense methods. With that in mind, the most useful application of this game is, as suggested by

[333] Curry and Price, 36–38.

the authors, for actual businesses that can base their attack and defense methods on security procedures.

Enterprise Defense is an example of why a higher level of technical fidelity is not necessary because the purpose of the game is for non-IT managers to be able to adjust their security processes to account for any holes in the attack methods. The very stream-lined representation of cyber in the game should, ideally, be enough to accomplish the limited intended goal. While the authors describe the game as "effects-based operations," the actual importance of learning from the game is focused on the potential holes or intrusion methods that *allow for* the effects. For instance, the players only need to specify what an attack is broadly, i.e. a virus that will run under the radar because it is newly developed, and then the effect, that the PC hard drives are wiped at the company.[334]

During the hot wash, the players are brought back together for an audit of the company, to see, out of all the defenses that were proposed, how many are being implemented. However, the question becomes what is the purpose of this game as opposed to penetration or social engineer live testing, which could offer more accurate information. Enterprise Defender offers a very low-resource and time-investment method of checking on the defenses of a system. The cyber expert would, ideally, have intimate knowledge of the business and be able to adjudicate with a higher rate of realism, not in regards to whether or not the attack itself will be successful because that is unknown, but whether the defenses and detection of that type of attack could be successful.

[334] Curry and Price, 36.

Entertainment Games

Commercial games, intended for education and fun, have a different function than sponsored, non-commercial games because the purpose of the game is less reliant on the application of any educational function and they are not 'experimental' in the sense of generating results for analysis. However, given the lack of available non-commercial games that focus on tactical or highly technical representations of cyberspace, they are useful for seeing alternative options for how cyberspace could be represented. Therefore, the game analysis for educational games will focus solely on the cyber component of the game and the potential utility.

Hacker: Steve Jackson

Steve Jackson's Hacker game describes the player as the "Net Ninja! Surf through the net, invading one system after the next."[335] The game is based on a Secret Service raid of Steve Jackson Games' Secret Service Raid, and therefore the ultimate goal of the game is to hack systems and avoid the Secret Service discovery.

Hacker represents cyberspace and computer systems tangibly as the 'board' of the game with 51 system cards that link together via cable hubs. Each card represents "a single computer system somewhere in the Matrix" and has nine potential features: shown below.

[335] Steve Jackson, "Hacker: The Computer Crime Card Game" (Steve Jackson Games, 2001).

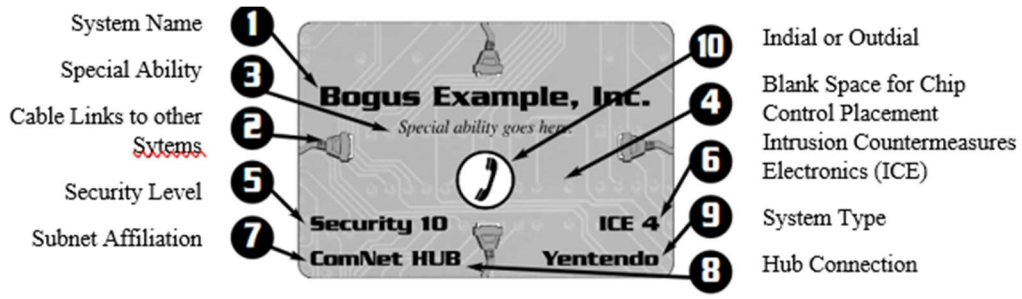

Figure 3. Bogus Example Card (Steve Jackson, "Hacker: The Computer Crime Card Game" (Steve Jackson Games, 2001).)

There are also 10 indial and 4 outdial cards, the former representing a that any regular phone can contact this system, and the latter representing that this system can phone other systems – the regular system cards do not have indial or outdial abilities. The game is set up using these cards depending on how many players; several regular system cards, from 5-14, and indial cards, from 3-4, are evenly distributed to the players. The players then build the system themselves by rotating in turn to

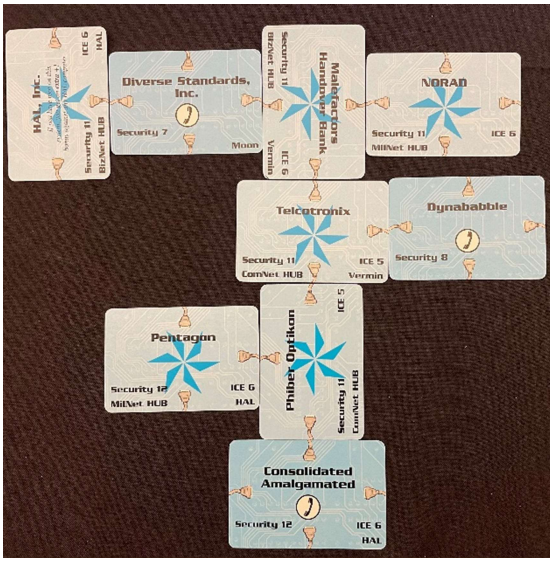

Figure 4. Sample Layout (Jackson.)

place down a card that links to another card. The only way a card can start a new system is if all connections have been used in the original 'net,' and a player can start a new net. An example system for a three-player game is shown below:

Interacting with these systems operates on a turn-based model. Each turn phase follows six steps:

1 Roll for Crashed Systems

A crashed system can be crashed by any player with root access during the 'phreak' phase of their turn, disabling it. At the beginning of each turn, a player rolls for each crashed system. A successful roll uncrashes the system and triggers housecleaning.

2 Housecleaning

During housecleaning, a system administrator realizes that they have hackers on their system and try to clean it. This can be triggered via five methods: uncrashing a system, when too many hackers are on one system, triggering an ICE, if a player narks during the Nark phase, or a player trying to self-clean himself off a system where they have root access.

3 Draw a Card

Draw a card from the set and play it onto the net or, if it is a card with a special ability, the card can be played or reserved. These cards will either be cards that grow the net or special cards.

4 Free System Upgrade

Skip the rest of the turn for a free system upgrade.

4 Hacking

There are three options for hacking into a system: a basic hack for access, an improved hack for root access once access is obtained, and a hack to remove other hackers once root access is obtained.

Each player beings with a certain number of hacks that can increase as their system upgrades from a basic PC/Plain clone.

Any indial card can be hacked from the on-set, but any other system must first have a path traced to the home computer. Other systems also have a secret indial code that, once discovered by a player, allows the player to treat it as an indial.

Hacks are done via rolling higher than the system's Security or ICE number, which earns basic access, but a high enough roll can earn automatic root access. A failure on a normal security roll is just a failure, but a failure on an ICE roll will result in detection, kicking the hacker off the system and the connecting system.

To draw a connection to a system can be done in two ways: either through the links represented on the cables or the hub. By hacking a hub, this is a one-way connection to all other systems in that net type.

5 Phreaking

Phreaking is making phone calls or sharing information, which can allow for cooperative gameplay, where hackers help other hackers gain access to a system they do not already have.

System crashing also occurs in this phase.

6 Narking

Narking is calling an administrator for a certain system, which requires a roll higher than the security number, but can also result in a self-raid if the roll is too low.

The timeframe for this game is difficult to determine, it is assumed to occur over several weeks or months – the only reference to time within the instructions is hacking, where "each hack represents many hours of persistent work, trying to defeat your target's security."

The goal of the game is to avoid being busted, which is a result of failing to avoid a raid via roll. However, the win condition of the game is active access to 12 systems.

Special Card Abilities

The modifiers can be sorted into two categories: human-related or cyber-related. The cyber modifiers include both software and hardware modifiers: viruses, building better equipment or using poor equipment, or system or equipment failures. Whereas, the human modifiers include either cooperative, such as finding allies or relying on personal connections, adversarial, such as being raided by certain government identities, or human error, such as sysadmin mistakes.

Cyber-Related	Human-Related
• Beelzebub Virus • Back Door • Disinfectant • Fuschia Box • Hack the Hacker • Hidden Indial • Ice Skating • Indial Busy • Mauve Box • Military Upgrade • Mona Lisa Virus • Reconfiguration • Self-Destruct • Slightly Off-White Box • System Upgrade • Taiwanese Modem • Wardialer	• Anarcho-Tech Marauder • Allies • Congressional Inquiry • Dad's a Lawyer • Divine Meditation • Get a Clue • Gooey Interface • Idiot Sysadmin • Local Police Raid • Secret Service Raid • Sysadmin on Vacation • Whoops • Bad Karma • Caffeine and Pizza • Caught Online • Combined Operation • Defense Intelligence Raid

• The Worm • Two System Upgrades • Uncrash • Disk Crash • Password File • Peek • Reply Hazy, Hack Again Later • Root Set to Default • Surge Protection Fails • Traffic Analysis File • Trashing	• Dummy Equipment • Early Warning • FBI Raid • Funding Cut • Hacker Hysteria • Hired by Telco • Original Manuals • Social Engineering

Even though hackers are playing against each other and they can help each other out, so the game is cooperative in a sense.

Modifiers to Hacking Bonuses:

- Net Ninja – Player with more active accounts on more systems than other players, bonus to hacking. The explanation in-game is that this bonus is because people will "tell you things."
- Same System Type – Controlling a system with root access that is one of the five types of computers in the game will grant a bonus to hacking a system of the same type.
- Sane Net Type: Bonuses for hacking a system on the same net (MILNet – military, ComNEt – communications, and BizNet – business).
- Adjacent Root Access – The game assumes that having adjacent access would allow for greater information espionage.
- Same Root Access – Another hacker can help a player trying to hack into a system they already have root access on.

[d0x3d!]

[d0x3d!] is a network security game that is a cooperative board game where 1-4 players interact as a group to collectively white hat hack a network to recover digital assets while remaining undetected.[336] The game visualizes the network as the board, with 24 square tiles that can be set up in various patterns, some of which are 'uncompromised,' 'compromised,' or 'hardened.' The game proceeds in a series of turns: the action turn – players can compromise a node, move to a compromised tile, exchange resources, recover a digital asset, or capture a node, the loot turn – where players draw resources, and the patch turn – where players draw patch cards which update tiles, kicking players out of nodes or out of the network.[337] Network patches include intrusion detection system, customer database, web server, client, single sign-on services, IMAP server, backup file server, wireless router, VLAN switch, VPN gateway, SMTP server, chat server, NAT device, network file server, certificate services, primary DNS server, sales database, secondary DNS server, VoIP server, firewall, client, or internet gateway.[338] The win condition of the game is to take back the four digital assets from the network: Personally Identifiable Information, Intellectual Property, Financial Data, and Authentical Credentials in partnership with your fellow hackers.

---

[336] Mark Gondree, *TableTopSecurity/D0x3d-the-Game*, TeX (2012; repr., TableTopSecurity, 2022), https://github.com/TableTopSecurity/d0x3d-the-game/blob/a4ea2e01cf631770c1c28290f024a75c56d6fbe1/instructions/d0x3d-rules-v2.pdf.
[337] Gondree.
[338] Gondree.

Game Utility of Cybersecurity Entertainment Games

These games are more technical than others, focusing on actual intrusion methods but at a level of understandability for non-cyber-experts. Hacker incorporates a hacking and information trade-off mechanics: helping a potential adversary could make a temporary ally or be detrimental due to information sharing. Given the very limited win condition, network exploitation, the level of technical detail is appropriate and can help non-cyber-experts understand the interconnectivity of the web and the impact of social engineering or human-related errors on network access and defense. [d03xd!] serves a similar purpose by understanding how patches and network updates can compromise the attack cycle. However, because both games are not technically representative enough as an accurate educational game for non-cyber-experts, nor is it suited for cyber experts, the utility of the game outside of an entertainment purpose is low. That being said, Hacker and [d03xd!] have the highest level of technical detail showing actual network intrusion and connectivity compared to other games that are more effects-based, and therefore the concept of representing network intrusion could be pulled for another game design. For instance, the increased specificity of these games applied to the Cyber Card Game from the UK could offer more nuanced intrusion methods or a more interconnected network representation. There is always a spectrum of abstraction to live penetration testing, and Hacker and [dx03d!] may represent the next step along the line for more technically-detailed or tactical level games.

Chapter 4. An In-Depth Analysis of Influence 2040 and Its Predecessors

Influence 2040 was a game sponsored by the Office of the Director of National Intelligence through the Virtual Student Federal Service. The goal was to build a wargame that modeled future intelligence warfare. Our design team was referred to Collect It All, an educational commercial game, which is based on Collection Deck, a sponsored educational game.

Collection Deck and Collect It All

Collection Deck is an originally classified, then declassified CIA training game, obtained by Mitchell Kotler and Douglas Palmer, through a FOIA request in 2017. This inspired the creation of "Collect It All" by Mike Masnick, a commercialized and updated version that received massive support on Kickstarter. [339] When the Virtual Student Federal Service requested a project on building a Future Intelligence Warfare Simulation, this was the game mechanics were originally based on. Therefore, the progression of mechanic and capability adaption throughout the iterations is useful.

Collection Deck

Collection Deck "is a training game designed to teach about various collection capabilities"[340] It is a card action-reaction type game. There are three types of cards: Collection Technique cards (GEOINT, HUMINT, MASINT, OSINT, or SIGINT) which correspond to the Intelligence Problem aspects it can be played against, Intelligence Problem cards (Political, Military, Economic, and Weapons), and Reality Check Cards

[339] Randy Lubin, "Diegetic Games | CIA Collect It All," 2016, https://diegeticgames.com/cia-collect-it-all/.
[340] MuckRock, "Materials for the Game 'Collection Deck,'" MuckRock, March 18, 2017, https://www.muckrock.com/foi/united-states-of-america-10/materials-for-the-game-collection-deck-35175/.

which affect the use of Collection Technique cards on an Intelligence Problem card. Each card has a short 1-2 sentence description, and the Collection Technique cards also explain what is unaffected by other factors (for example, Gray Literature – the collection of foreign open sources that are difficult to get to, are not affected by a media blackout).[341] The Reality Check Cards add a matrix element to the game, where some cards will require players to explain how the Collection Technique could play out in the real world. Most of the GEOINT (Satellite) cards are redacted – with the few available being non-high-tech items (taking photos of items of interest), more HUMINT items are available, again being non-tech related, such as using diplomats or deploying forces. MASINT has one card on biometrics, which gives a general description. OSINT has several capabilities available, but while some use technology, all are general as well, such as using commercial databases or foreign material translations. SIGINT is where the most non-redacted technology-related capabilities are available: Computer Network Exploitation, four satellite connection cards that collect different information COMINT on foreign voices, foreign transmission geolocation, radar signal collection, and military system telemetry collection. Out of 66 Collection Technique cards, 27 are available.

Cyber-Related Techniques:[342]

Category	Name	Description
GEOINT (Satellite) Technique	N/A	Private companies collect medium and high resolution black and white imagery
GEOINT		Human collections and sources can take pictures of places or activities of interest
HUMINT	Foreign Material Exploitation	The acquisition of foreign equipment or technology for intelligence purposes

[341] MuckRock, 23.
[342] MuckRock, "Materials for the Game 'Collection Deck.'"

HUMINT	Document and Media Exploitation	Captured documents and electronic media can provide many intelligence insights
OSINT	Foreign Media Transcription	English-language foreign media products can be provided directly to the IC without translation
OSINT	Foreign Media Translation	The translation of openly available foreign media sources
SIGINT	Computer Network Exploitation	Accessing a foreign computer system remotely or through the physical access system
SIGINT	COMINT Mapping	Satellites can geolocate foreign transmissions
SIGINT	Overhead COMINT	Satellites monitor and collect foreign voice and data communications
SIGINT	Overhead ELINT	Satellites collect signals from radar and electronic warfare systems
SIGINT	Overhead FISINT	Satellites collect data transmissions associated with testing military systems

The Reality Checks disable a certain category of intelligence collection types. Bad weather, Satellite Warning counter GEOINT, Encryption counters SIGINT, Satellite Failure and Ground Station failure counter both. Re-assigning Linguists counter SIGINT and OSINT, while others such as denial, red tape, and competition counter multiple or all collection techniques.

Cyber-Related Reality Techniques: [343]

Counter		
GEOINT Satellite	Satellite Warning	Let's give a hand to all those amateur satellite watchers
GEOINT or SIGINT Satellite	Satellite Failure	How much did we pay for this thing again?
GEOINT or SIGINT Satellite	Ground Station Failure	The satellite is working, we just can't talk to it
MASINT	Corrupt Signature Database	Did you try rebooting it?

[343] MuckRock.

SIGINT	Encryption	Xcvx a2sdf rf436 79->/a
OSINT	Disinformation Campaign	But you know that I know that you know that I know, so…
OSINT	Media Blackout	I'm sorry, our offices are currently closed

The Intelligence Problems are wide, general items, such as North Korea Nuclear Talks or Chinese Yuan Evaluation. They feature a difficulty level on a scale with 3 being the lowest, for issues like Macedonia Ethnic Violence and 9 being the highest.

CIA Collect It All

CIA Collect It All is very similar to the format of Collection Deck. It pits one player, using *technique* cards to overcome a *crisis,* while other players attempt to interfere with *reality checks.* To account for the redactions in the original material, the techniques are supplemented by research from Techdirt, Diagetic games, and the AH Games' version. However, in the same vein as the Collection Deck game, a more appropriate characterization of the game is as a player versus environment/system game, rather than player versus player, because the adversarial other 'team' operates as 'reality' obstructing player goals, rather than as an active equal entity.

Cyber-Related Techniques:[344]

GEOINT: Airborne Imagery INSAR RF Communication Mapping Commercial Multispectral Imagery *Commercial Grayscale Imagery*	HUMINT: *Document and Media Exploitation* *Foreign Material Exploitation*	MASINT: Biometrics IRINT Airborne Missile Tracking Multi-region Signature Library International Monitoring System RADINT	OSINT: Darknet Databases Commercial Databases *Foreign Media Transcription* *Foreign Media Translation* Internet (Analysts do their own open-source research)	SIGINT: Voice Interception DNS Hijacking COMINT Mapping *Computer Network Exploitation* Text Interception Trojan Horse – USB Drives

[344] Lubin, "Diegetic Games | CIA Collect It All."

Defense Support System *Handheld Imagery* Visible Remote Sensing Infrared Remote Sensing LIDAR Remote Sensing Time-History Analysis Photogrammetry Georeferenced Social Media Unsecured Network Cameras Vibrometry				Telecom Coordination *Overhead COMINT* *Overhead ELINT* *Overhead FISINT* Signaling Channel Interception Listening Post Spear Phishing

Cyber-Related Reality Checks: [345]

Counter	
HUMINT	Aggressive Counter-Intel
GEOINT	Satellite Warning
GEOINT or SIGINT	Satellite Failure
	Ground Station Failure
MASINT	Corrupt Signal Database
SIGINT	Encryption
OSINT	Disinformation Campaign Media Blackout

The main gameplay difference is that there are now resolution reality checks, which include a required explanation of how to use a technique, and success or failure that is narrative-related, such as political blowback, career risk, or recruiting new assets that can be incorporated into gameplay. As can be seen by comparing the two games, the

[345] Lubin.

reality checks remain very similar, and the Cyber-related Techniques, while expanded, still fall into surveillance-built measures. However, Collect-It-All features more unclassified hacking abilities, suggesting a more combative usage of cyber warfare.

Influence 2040

Influence 2040 was designed by the 2019-2020 Virtual Student Federal Service Office of the Director of National Intelligence Team, and the design process and considerations are as follows.[346]

Purpose, Sponsor, and Participants

Influence 2040's goal was to look at intelligence warfare in the future to educate and get analysts thinking about the potential challenges that technology could present. This fits into the purpose of teaching cyber concepts, but also for speculation on future technology capabilities and scenarios, with the ultimate purpose of education. The sponsor parameters were very minimal, but we knew it has to be a game that was developed to be played both in-person and virtually, given that we were a virtual design team. The final, official design goal published in the rule book is: "The game is meant to be a competitive strategic storytelling game to help intelligence analysts forecast what unique challenges lay ahead in the next 20 years."[347]

We knew that, ideally, this would be used as a training game for analysts in the Office of the Director of National Intelligence, and therefore address intelligence analysts. Implicitly, it was also assumed that the game would need to be short enough to be run in a couple of hours, maximum, that adjudication would not need an expert, given

[346] Sarah Chen et al., "Influence 2040 Rulebook," June 5, 2020.
[347] Chen et al., 2.

that none of us were experts in technology or intelligence collection methods, and that the game itself would be built for non-cyber experts, and therefore not require a high level of technical detail.

Game Format and Scenario[348]

Influence 2040 is a two-sided, narrative card game that plays with 3-12 players and 1-2 game masters, one to handle the scoring and one to handle the narrative elements. It pits a challenger country against a target country in a battle for intelligence and influence. There are four fields of control: political, economic, technological, and social, each with its own level of vulnerability and pressure that can be raised or lowered by playing the card capabilities. The game is won by capturing fields of control, a field is captured by the Challenger country by raising the pressure to above 10 or by the Target by lowering the vulnerability to 0. Capability cards are played using resources and specify the field they affect. There are eight stages of the game that encompass one turn, and five turns in the game.

> "Stage 1: The Destabilizing Event - Using only covert capabilities, the Challenger lays out its opening move. (Note: After Round 1, the Challenger can use overt capabilities in this stage).
>
> Stage 2: Reactions - Target fires back. Using either overt or covert moves, the Target responds to the Challenger's actions.
>
> Stage 3: Up the Ante - Challenger escalates the situation. Now, using either covert or overt capabilities the Challenger makes its next moves.

[348] Chen et al., 3–5.

Stage 4: The Last Word - Target has a final chance to respond. The Target has the last move before scoring begins and can use covert or overt capabilities. Target can request US assistance in this stage.

Stage 5: Scoring - Points are tallied and any variable effects are determined.

Stage 6: Consequences - If either team went over their resource total, a die is cast to determine what consequences occur, if any.

Stage 7: Environmental Shifts - An Environmental Factor card is revealed that adds to the narrative for the following round.

Stage 8: Ripped from the Headlines - The Game Master relays the overt events and environmental shifts to each team, changes the scores according to the overt and covert events, declares if either side has won a field, and announces any changes to resource points. The round is then over and Stage 1 begins again."[349]

If the Challenger country has not captured three or more fields by the end of the turns, then the Target country automatically wins. The game was built in this way to favor the Challenger country playing aggressively, and the Target country's goal being survival and sustainment of stability, reflective of how information warfare occurs in the modern day – with propaganda campaigns targeting the U.S. and European countries often being predominately one-sided.

Cyber Capabilities

Influence 2040 is a cyber-in-game, rather than a cyber wargame because capabilities support the ultimate goal of intelligence and influence competition and because the majority of capabilities are not 'cyber' or 'technology-focused. Most of the

[349] Chen et al., 5.

capabilities presented are ones that either exist or can be extrapolated out as fixed capabilities: a mix between present and future capabilities.

The cyber operations are represented on an operational level, to fit into an overall influence warfare campaign, and cyber capabilities are both covert and overt. The game runs on two channels, an overt narrative channel, and a covert channel for both countries. There is very little representation of the cyber attack and defense cycle on a technical level. The representation of cyber is effects-based, which is also how the capability development worked. We asked questions based on what we wanted to be accomplished by the particular capability and tried to speculate how new technology could reach that goal. For instance, if we wanted to collect audio data, how could nano-technology be used? If we wanted to sort through information collected, how could artificial intelligence be used? The thought process behind deciding on an effects-based capability was on the purpose of the game. The intelligence analysts are not concerned about how nano-technology works, or what AI algorithm needs to be deployed. Instead, cyber capabilities are a supporter.

There are no 'response' capabilities directed towards blocking certain capabilities, unlike the CIA and Collect-It-All game. With those two, there were 'environmental' cards that players could use to block certain capabilities – for instance, SIGINT technologies could be blocked by a ground station failure. However, the only way of opposing teams can block each other's capabilities is through 'argumentation' mechanics, by exploiting a lack of sufficient explanation and realism in the former team's argument, or by trying to argue against it.

The influence and intelligence warfare capabilities that are related to cyberspace and technology are listed below:[350]

Purpose	Overt/Covert	Action
Preposition	Covert	Production Line Intervention Spyware in a technical device before it is delivered to the target.
Preposition	Overt	Digital Citizen Protection Privacy and transparency enforcement, regulated advertising, various platform controls.
Preposition	Covert	Malware Insertion Via Hardware and Software Updates Place spyware in a technical device or its updates before delivery.
Collect Information	Covert	Crowdsourced Reporting Local observers post bits of conversation that AI synthesizes into meaningful reports.
Collect Information	Covert	Personabot Phishing Bots develop intimate relationships to elicit identifiers that allow entry to accounts and systems.
Collect Information	Covert	Emotional Reading Detect change in emotional state and decision proclivity with detectors near individuals
Collect Information	Covert	Nano-scale Multi-spectral Listening Post Low-observable device collects wi-fi and many other signals simultaneously and misdirects identification scans.
Collect Information	Covert	Deep Person Surveillance via Phone A useful download gains access to full phone sensory capabilities when unread Terms and Conditions are accepted.
Collect Information	Overt	Financial Surveillance of Public Trust Personnel

[350] Sarah Chen et al., "Influence 2040 Card Capabilities," June 5, 2020.

		Identify personnel receiving illicit payments from foreign influence agents.
Collect Information	Overt	Trace and Track Social Media Posters of Interest Track IP, place and lock roaming digital and satellite surveillance to the person.
Collect Information	Covert	Multi-Signature Collection from Emitting Mechanisms Robots, printers, cars, etc. emit data that can be interpreted.
Collect Information	Overt	Biometric Sensors Locate and track specific persons and changes in movement, health, or mood.
Collect Information	Covert	Communicating Tattoo A temporary, near-invisible e-tattoo allows an asset to convey sensitive information to handlers without close contact or intercepted signals.
Exploit Information	Overt	Interpret Leadership Tells Combined analysis of video and audio recording of Challenger leaders to detect decision changes.
Exploit Information	Covert	Artificial Intelligence for Big Data Use AI to draw sense from massive flow.
Exploit Information	Covert	AI For Big Data Drawing intelligence from massive records that would be otherwise unavailable.
Exploit Information	Overt	Real-Time Crowdsourced Mapping Protesters can keep moving and avoid clashes with the police.
Exploit Information	Overt	Remote Viewing Using a Virtual Reality headset, simulate walking through remote locations based on many recorded and real-time inputs.

Exploit Information	Overt	Real-Time Auto-Reporting and Analysis AI runs the intelligence cycle without delay and approximates instant commentary.
Undermine Adversary	Overt	Detect and Remove Disinformation on Social Media Platforms and News Sites
Undermine Adversary	Overt	Persistent Cyber Engagement Preemptive engagement in active cyber-warfare against foreign targets.
Undermine Adversary	Covert	Deepfake Online Personalities Extremely realistic, but phony videos and images create fake statements.
Undermine Adversary	Covert	Realtime Self-Organizing Protest Crowd Communications-enhanced crowds can be enlisted to resist foreign incursions. Digital Evasion Tactics Evade standard online techniques for identifying foreign influence activities.
Undermine Adversary	Covert	False Video Substitution Superimpose a different face into videos to create a proof of false events.
Undermine Adversary	Covert	Deepfake Online Personalities Extremely realistic but phony videos and images.
Undermine Adversary	Covert	Search Engine Spoofing and Biasing Tricking search engine algorithms to promote false pages and demote reliable pages.
Undermine Adversary	Covert	Coordinated Fightbots Generate polarizing conflict from both sides of a dispute.
Undermine Adversary	Covert	Media Flooding Disrupt discussion and the search for truth by flooding the media with disorientating content.
Undermine Adversary	Covert	Fake Local Media Outlet Use social media to create fake local media outlet accounts.

Disable Adversary	Overt	Distributed Denial of Service Use DDOS attacks to disrupt key functions.
Disable Adversary	Overt	Mesh Network Unblockable, untraceable pop-up network for use by dissidents during collective action.
Disable Adversary	Covert	False Warnings and Alerts Reduce effectiveness of alerts on real incursions and emergencies.
Disable Adversary	Covert	Financial Encryption Use crypto-banking and multiple money transfers to evade detection.
Disable Adversary	Overt	Anonymized Face and Voice Can deliver authentic messages without disclosing a person's face or other identifying characteristics.
Disable Adversary	Overt	Localized Electromagnetic Pulse (EMP) A directed pulse knocks out area electronics momentarily.
Disable Adversary	Overt	Quantum Communication A limited volume of data cannot be intercepted. Quantum-resistant Encryption A limited amount of data cannot be decrypted, even with quantum algorithms.
Disable Adversary	Covert	Quantum Decryption Quantum algorithms get plaintext from conventionally encrypted materials
Disable Adversary	Overt	Confusion Patch to Block Facial Recognition New technology counter attempts to track citizens.
Disable Adversary	Covert	Deny Access to Technology DDOS attacks are used to shut-down key infrastructure.

To play these capabilities, players must utilize argument mechanics and make a compelling argument as to how these attacks fit into the overall narrative and why the other country is vulnerable. Adjudication is solely reliant on the game master's decision and includes no chance elements.

Testing and Iteration

We played four full run-throughs of the game, which were done asynchronously. Similar to an online version of Diplomacy, we gave people a full day to discuss with their team before making their overt and covert moves.

This helped us find out during earlier rounds that players would start 'playing the game' rather than 'wargaming' in the sense that they would play to the game mechanics – calculating the trade-off between resource investment and pay-off because we quantified the effect that capabilities could have. Therefore, we added more power to the game master to adjudicate, to try to balance out the cost, potential effect, and actual effect that would force players to think more about how the capability could be used rather than doing basic maths as a key part of taking their role. We did not build in any 'chance' rolls into our game. Instead, adjudication to determine success was entirely up to the game master, rather than modifiers for rolls to determine the success of a certain cyber campaign.

Data Generated

Given the remote nature of the internship, all games were played online. We have the text of covert and overt channels available for what moves were pulled. We, unfortunately, did not retain the discussions that happened between teams because most of those conversations were held online. However, if this game was run analytically,

wargames use recording devices or live note-takers to try to capture the human decision-making process.

We did find two common threads: players were more risk-averse during earlier turns and more risk-tolerant in later turns; 'target' countries attempted to play more 'fairly' in earlier rounds and then devolved into playing as 'dirty' as the 'aggressor' countries in later rounds. We also found that overall, the narrative structure of the games looked very much like influence warfare today – the technology did not create any radical new methods of influence and intelligence warfare, it just acted as an enhancement to what was already available. While these findings are not indicative of cyber conflict and influence warfare and cannot be detached from the game design to apply to the real world, it does give an interesting example of what a similar context, but with an analytical purpose, could find. It also, however, poses the concern that these threads are what the players will take away from the game, rather than sparking thought as to how new technologies could expand intelligence collection methods.

Chapter 5. Limitations of Cyber Wargames and Recommendations Moving Forward

The representation of cyber poses limitations for the utility of cyber wargames, and sometimes the solution to these limitations is an acceptance that wargames are an imperfect representation of one instance of possibility.

The representation of cyber capabilities is a guessing game.

The same reasons that cyber is difficult for decision-makers to understand also make designing cyber wargames difficult.

Limitation: Cyber capabilities are constantly changing, and there is no standardization of abstraction.

The difficulty in designing wargames because of abstraction is well-documented as a concern, but the complications of cyber itself make designing cyber wargames a uniquely challenging endeavor. In "Pathologies of Obfuscation: Nobody understands cyber operations or wargaming," Kollars and Schechter lay out the "confounding characteristics of cyber… the environment and cyber tools" that rapidly shift.[351] The authors worry that the abstraction of cyber in games, without expert agreement regarding both 'real' cyber and a standardized method of abstraction, is not meaningful. The churn of hardware and software combined with the "human (in)comprehension of technological churn – the constant updating, upgrading, replacing reformatting, repurposing, and modifying – can create new vulnerabilities and new kinds of attack." Due to the constantly changing

[351] Nina Kollars and Benjamin Schechter, "Pathologies of Obfuscation: Nobody Understands Cyber Operations or Wargaming," *Atlantic Council*, February 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pathologies-of-obfuscation-nobody-understands-cyber-operations-or-wargaming/.

nature of the cyber domain, Kollars and Schechter analyze it as akin to "declaring that the ocean might be ice for the next three hours but then dry up entirely for twenty minutes" (i.e. movements in cyberspace may free flow until a sudden and devastating DDOS attack) or "ships moving on the water's surface will inexplicably sink or teleport to the other side of the Earth" (i.e. an attack can randomly fail for an unknown reason or ricochet far beyond its original intended effects).[352]

Potential Solution for Non-Standard Abstraction: Attempt to model and disseminate "standardized templates for cyberspace operations."[353]

Connections Wargaming, an annual conference, brings together wargamers from different industries and agencies, with presentations and workshops. A working group composed of expert designers could attempt to analyze current conceptualizations of cyberspace operations and create a standard level of abstraction and representation, based on the technical level need of the game, as an open-source resource for designers. However, this still runs into the problem of a useful abstraction – just because the abstraction is potentially standardized does not mean it is a useful representation. Game purposes and scenarios are unique enough based on the sponsor request and desired information that standardization of how to represent cyber would likely not be useful. Unlike military units, which are typically represented by units on a hex board, or artillery fire, which is typically adjudicated via a dice roll for accuracy and hit, cyber attacks and defenses are so varied that anything other than a guideline on what representations are possible would likely not be heeded.

---

[352] Kollars and Schechter.
[353] Kollars and Schechter.

Potential Solution: Create and analyze a repository of cyber wargames to find common trends in cyber representation.

There are few available cyber wargames to the public: The Center for Naval Analyses rotates reports available, RAND has a slow publication time, and IDA does not publish many reports for public view. A consolidated repository of cyber wargames could be a resource to see what methods other designers are using to find a preferred mechanism of representation. But even in the games reports observed in this thesis, there is no common representation of cyber capabilities – each game approaches cyber in a different way and includes different capabilities on different levels of warfare.

Limitation: Cyber capabilities are classified, and abstracting down to unclassified information poses a challenge because of limited information.

Cyber gets classified very quickly. Even if you build an unclassified wargame, they will add details that make it classified, which also makes it more useful.[354] The technology itself, the hardware, software, and end networks, are generally open-source because everyone uses the same systems – just run-on classified networks. However, how capable and who has what offensive versus defensive cyber operations are heavily guarded.[355] This issue returns to the original complication with making decisions in cyberspace; there is no overview of its current state. If adversaries become aware of existing capabilities, and details regarding those capabilities, this could result in a direct reduction of military or cyber competitiveness. There is no upside to information sharing when it comes to cyber capabilities. No unclassified cyber wargame can or should

[354] Interview with Unnamed Source.
[355] Interview with Unnamed Source.

accurately represent current cyber capabilities because a large part of the cyber advantage is secrecy.

Classification also blocks the contextualization of the problem. As Bartels writes, analytical wargames "do not validate when used independently of other analysis."[356] When cyber wargames happen in a vacuum, behind closed doors, they remain cut off from not only real-world application but also real-world analysis. This lack of real-world information is an issue when designing a game, particularly an analytical game. In particular, for future-facing games involving situations where there still exists no real data, Bartels claims that "we are much better off when we try to learn from wargames, rather than prove with wargames."[357]

Potential Solution: Build cyber wargames with less specificity at lower classification levels.

CNA, when building games that are intended for lower classified levels, works with people that understand the nuances of classification levels to verify what can and can not be included.[358]

> "You have to make assumptions, and you hope you're not wrong. You talk to people who do know the information to decide which assumptions are the ones that you can and should make that are consistent with higher classification without revealing that. This essentially means that you go into fewer significant

[356] Elizabeth Bartels, "Getting the Most Out of Your Wargame: Practical Advice for Decision-Makers," November 19, 2019, https://warontherocks.com/2019/11/getting-the-most-out-of-your-wargame-practical-advice-for-decision-makers/.
[357] Bartels.
[358] Sepinsky, Interview with Jeremy Sepinsky.

digits on your answer. You reduce specificity, but that doesn't change what you're talking about."[359]

There is currently no good solution to the classification issue other than acceptance that unclassified wargames will be best guesses, and so will the outcomes of those games.

Limitation: Cyber wargames can oversimplify, particularly with fixed capabilities. Fixed capabilities within cyber wargames can teach or model a false action-reaction dynamic.

Cyber space has far more capabilities than you could ever reasonably build within a game Creating cards representing tank models gives you a smaller card deck compared to trying to name every code you could throw at a firewall. Wargames often resort to high-level strategic effect capabilities. Or, even if specific capabilities are built out, it creates a false 'action-reaction' response spectrum: Anti-tank missiles to tanks are not the same as a Faraday Cage to an EMP Jammer. This problem is evident in games with capabilities that have cards that directly interact with each other.

This is up to the designer to attempt to avoid unless they find the benefits (a clear example of cyber actions can counter one another) outweigh the negatives, the adjudicator to address during the follow-up after the wargame, or the analyst to recognize when trying to establish a causal relationship in the game.

[359] Sepinsky.

Limitation: Cyber wargames can overcomplicate through technical jargon.

Cyber wargames only need a certain amount of information and mechanics to accomplish their purpose. However, to improve the fidelity of the game or to make it feel more realistic, designers can add unnecessary levels of technical information. Again, this runs down to a design judgment; but, it is worth mentioning when analyzing the design of other cyber wargames.

If this game were to abstract further or remove the technical details and become more accessible to non-cyber experts, would the wargame purpose be better accomplished through the increase in its participation pool or player understanding?

Limitation: Cyber experts have different conceptions of cyberspace, and therefore subject matter expertise can be unreliable.

Wargames ultimately rely on player buy-in and understanding in an incredibly complex field. Kollars and Schechter describe the field as "federated and highly jargonized." The language used can range from a policymaker's level of understanding to a highly technical coder expert's.[360] Thus, a reliance on experts falls into two major issues: experts disagree, and therefore adjudication for a game can differ based on the expert. As previously mentioned in notes on game design, adjudication typically happens either by the 'white cell,' by 'luck,' or often a combination of the two. Curry and Price raise concerns regarding the use of experts, noting that: "games must rely on 'experts' in name only, anointed in some way by background or media exposure. The danger of

[360] Kollars and Schechter, "Pathologies of Obfuscation."

agenda-driven self-fulfilling prophecy is obvious."[361] If experts are wrong, then the adjudication is wrong.

The internal validity of the wargame can be affected by the consistency and knowledge of the adjudicators, not just the participants. This holds particularly true for wargames that require adjudicators to moderate success probabilities, explain the possible and impossible, and decide outcomes. The security clearance divide between technical understanding can also become a barrier when it comes to expert adjudicators.[362]

Potential Solution: More public-private integration and information sharing is needed to create more reliable experts with a better overview of the whole picture. *Cyberspace does not exist in two separate hemispheres of private and public infrastructure, and, therefore cyber experts should not be within ivory towers as well. Sharing knowledge without crossing classification barriers should be pursued in the future as more cyber expert generalists, rather than specialists, are needed.*

Potential Solution Overall to Cyber Representation: Accept that unclassified, and even classified wargames, cannot accurately represent cyberspace and the cyber attack-defense dynamic. Reframe the conception of cyber wargames.

The listed difficulties in accurately representing cyber capabilities are only problems if a sponsor is trying to get a predictive value or an analytical value that relies on a single outcome out of a cyber wargame, and therefore the sponsor and designers are worried about 'getting it wrong.' There needs to be a reframing and emphasis of cyber wargames as exploring *one potential outcome* based on *one potential conceptualization*

[361] Curry and Price, *Dark Guest Training Games for Cyber Warfare*, 22.
[362] In this interview, Curry meCurry, Interview with John Curry.

or educated guess of cyberspace capabilities. This means that for educational games and analytical games to create useful data, we need to build and run more games with more variations.

Next Steps: Build iterative wargames that can adapt to new information.

One run of a cyber wargame explores one possibility. Therefore, for better data and education, cyber wargames should be re-run and should have dynamic endings so players can see how their decision-making impacts cyberspace. The 2019 Defend Forward report notes that wargame iteration may increase the reliability of the insights derived from the game. To return to Admiral Nimitz's remark during WWII on almost nothing in the war being a surprise *because* of the constant wargames in the Naval War room, running wargames once with the same group of participants is not utilizing the full value of wargaming. Oftentimes, wargaming is run once, not multiple times with the same participants, because of time constraints, and other limitations (financial, building the game itself, the ability for the facilitators to gather and organize the contestants.)

Imagine a situation like a decision tree, where players are presented with two options, choose one, leading them to another two options, choosing one, and so on and so forth. One wargame run will explore one line out of the decision tree due to player actions and reactions, but this outcome is often not representative of the 'best actions taken' which is why wargame value is derived from 'lessons learned.'[363] However, to

[363] This framing of a decision tree is credited to Professor Ran Libeskind-Hadas, who I spoke with during a mock interview where he raised the criticism that wargaming only ever shows you one potential path, leaving potentially hundreds or thousands unexplored. Ran Libeskind-Hadas, Conversation with Professor Ran Libeskind-Hadas, November 16, 2021.

truly get to the heart of wargaming's value, participants should play once, realize mistakes, and then play again to achieve a 'better' outcome or event to experiment with different methods that may originally present as absurd. If we view wargames as a consequence-free way to test and learn, then the testing aspect is wasted if we only test once.

St. Paul Syndrome I and II were two wargames played in 2020 and 2021, in a collaboration between the Los Alamos National Laboratory's Office of National Security and International Studies and the Center for Strategic and International Studies. They explored a pronged scenario, where a mysterious virus appeared, the US was accused of sinking a Russian ship suspected of ferrying biological warfare materials to North Korea, and tourists with North Korean ties visiting St. Paul recently before the infection began. While cyber was not predominant in this game, there was the use of misinformation warfare. However, an important takeaway from this particular game is that it was deliberately iterated. St. Paul I and II are the exact same scenario, kept under wraps, allowing the game to be played with new player groups in its second iteration St. Paul Syndrome II: "even when running the same scenario with participants of similar professional backgrounds, we see teams take a wide variety of strategies and actions."[364]

That being said, iteration may be dependent on the *purpose* of the game. TTX (table-top games) are, according to Ian Williams, deputy director for the CSIS Missile Defense Project are "experiential learning tools… [with] limited ability in predicting how states might behave in a given situation," however, they are useful to "shake out new

[364] Virginia Grant, "Wargames," *Los Alamos National Laboratory*, July 26, 2021, https://discover.lanl.gov/publications/national-security-science/2021-summer/wargames.

questions and possibilities that have not been considered."[365]Other participants in the wargame noted that the valuable part of the exercise was learning how nuclear weapons could be used to 'flex' or their application in non-conflict scenarios. In other words, the value in this particular wargame was education, but it was also *exploration*, which requires iteration with multiple groups rather than a singular focus group of non-multidisciplinary experts or policy-makers.

However, given that the resources for running a game are not infinite, sponsors and analysts must choose how many times to run a game or iterate a game. Bartels proposes two ways of looking at repetition: sampling and saturation.[366] Sampling addresses looking at the iteration mechanic in the same sense as surveys, trying to use larger samples for more validity regarding generalization. However, this runs into the issue of participant selection where, unlike academic surveys or studies that can use the general public or a subset, the number of cyber experts, dedication to game time, and availability of schedules poses a much higher barrier. There is difficulty getting the right people into the room all together in the first place, let alone finding more people at the necessary level of expertise and coordinating schedules multiple times. The second way of looking at the value of iteration is saturation, where the game should be run as long as it keeps turning up different results.[367] Bartels notes that saturation may lead to very little

---

[365] Grant.
[366] Elizabeth Bartels, "Incorporating Gaming into Research Programs in International Relations: Repetition and Multi-Method Analysis" (ISA Annual Conference, April 8, 2020), http://www.elliebartels.com/uploads/1/1/0/6/110629149/bartels_multi_method_games_8april2021.pdf.
[367] Harry Wolcott, Sarah Baker, and Rosalind Edwards, "Introduction," in *How Many Qualitative Interview Is Enough? Expert Voice and Early Career REflections on Sampling and Cases in Qualitative Research* (National Centre of Research Methods,

need to run a game: "If the purpose of the game is to scope follow on research, and the 80% solution is enough to inform next steps," while "for more poorly understood or complex problems, repetition may be an important way of building understanding."[368] However, because most wargames are not iterated in the first place, wargames are reaching a low utility and saturation rate.

Rather than running the same game in iterations, wargames can also focus on updating or changing their original assumptions. When wargames are designed for a sponsor, they are often bespoke. However, games can keep the same mechanics and create new cyber capabilities as new information is released or a new scenario of interest develops. SIGNAL "is specifically designed to allow for the flexible introduction of treatment variable types."[369] MERLIN and Littoral Commander allow the swapping out of different scenarios. This extends the utility and saturation value of a wargame because it can test new information without having to build a new framework.

Rewind time within wargames.

If a cyber wargame begins with placing the player in a theoretical scenario (theoretically regardless of whether it's a realistic or fictional scenario because of the uncertainty regarding cyber), and wants to see where the player will end up after making the decision, it can introduce a 'rewind time' mechanic. If you have ever read a choose-your-own-adventure book, there is the 'correct' way to play through the book, which is to run

---

2012), 4; Bartels, "Incorporating Gaming into Research Programs in International Relations: Repetition and Multi-Method Analysis."

[368] Bartels, "Incorporating Gaming into Research Programs in International Relations: Repetition and Multi-Method Analysis."

[369] Goldblum, Reddie, and Reinhardt, "Wargames as Experiments."

through the entire adventure, flipping along to the pages corresponding with your decisions, until you reach your end. However, if you want to replay the book and reach a new conclusion, you can play the cheater's version by flipping back through the book to find where you went wrong. Cyber wargames can operate with a similar mechanic, where a derailment can allow for creation by rolling back decisions and adjudications rather than continuing on a losing path.

Sponsor requests, game format, and design can be limiting.

Problem: Sponsors ask the wargame to do too much, or to verify or predict an outcome.

> "Humans are miserable constants in an experiment, and they're terrible at predicting even their own behavior, let alone the behavior of complex systems. You'll see an eye twitch whenever we hear 'the wargame predicted, the wargame validated.' As soon as we hear the 'v-word,' we're outta here."[370]

Wargame questions must be deliberate because it shapes the design and ultimate result analysis. As Bartels notes, broad questions will help find new questions for the future, while more targeted questions will give more focused answers.[371] This is not to say that wargame questions need to be *narrow,* but they need to be formed for a specific purpose. For instance, the Cyber Storm series games have a long list of goals and objectives and may serve too many purposes. This might be a root cause for why the Cyber Storm findings are so general, the simulation cannot address one specific issue.

---

[370] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[371] Bartels, "Getting the Most Out of Your Wargame: Practical Advice for Decision-Makers."

Kollars and Schechter propose that games may be "potentially on safer ground when remaining constrained to a narrow set of agencies…instead of attempting to chase the most realistic scenario."[372] Another method is to "focus less upon the specific quantitative realism…and instead proceed openly in dialogue with cyber adjudicators working directly with players as the game progresses."[373]

The sponsorship process is also complicated by a limited lack of knowledge on the sponsor side. There is the process that wargamer designers would like to happen, and what happens.[374] Noted by several wargame designers, often the sponsor does not have a background in wargaming. This can be attributed to inexperience, and also through the cycling system of military postings, where officers rotate. Therefore, wargame designers will work with different officers even when sponsored by the same branch or unit of the military.[375]

However, Sepinsky believes that sponsors not having expertise in wargaming is not a detriment, it is why they outsource to FFRDCs to build games. CNA is providing the wargaming expertise, the sponsors are providing the questions.[376] Building trust with a sponsor is crucial so they look at you as a wargaming authority because the design needs to be a back-and-forth conversation. If sponsors do have expertise in wargaming, it is typically as attendees or sponsors, not as designers and analysts.

---

[372] Kollars and Schechter, "Pathologies of Obfuscation."
[373] Kollars and Schechter.
[374] Bartels, Interview with Elizabeth Bartel.
[375] Sepinsky, Interview with Jeremy Sepinsky; Bartels, Interview with Elizabeth Bartel.
[376] Sepinsky, Interview with Jeremy Sepinsky.

Potential Solution: Sponsors may need more guidance during the wargame question development process*. Cyber wargaming is a relatively new discipline, and therefore sponsors may have unrealistic expectations as to what a game could accomplish. There are requests that a wargame is not suited for, for instance, "wargames are bad at generating hard numbers; hard numbers are inputs, not outputs.*[377]

Problem: "Integrating cyber defense effectively into strategic and operational level wargames is very difficult."[378]

Cyber defense is a "boutique" part of the industry, and it is hard to represent that within a game – there are mechanics like creating prioritization systems or marking systems players want to defend, but because cyber defense happens in varying degrees constantly, there is no good way to abstract it in a way that is impactful to the game and realistic. However, more experienced players will notice if cyber defense is missing.

Potential Solution: Some games will create modifiers on attack success-burn rolls that try to incorporate cyber defense. *Littoral Commander, for instance, has a mechanic that affects the probability of cyber attacks based on previous successes and failures. However, most games just focus on the attack cycle rather than the defense portion. If defense is not relevant to the purpose of the game, this can be disregarded.*

Problem: Psychological effects cannot be accurately replicated in cyber wargames.

Game design cannot create the psychological effects that impact the speed of making decisions and the risk associated with them.[379] Nor can the control cell adjudicate

---

[377] Marrin, Vogt, and Pellegrino, Interview with Don Marrin, Jason Vogt, and Peter Pellegrino.
[378] Marrin, Vogt, and Pellegrino.
[379] Marrin, Vogt, and Pellegrino.

psychological pressure. “I can’t call a player's cell and tell them that they’re uncertain or worried, it has to be an internal experience based on what the game has created.”[380] Marrin, Vogt, and Pellegrino present an example where a leader’s family is being threatened, and the ‘leader’ is notified through internal access to their private cell phone. Players know that their ‘real-world’ families are not at risk, and therefore their calculus on decision-making is not affected in an intended way.

This is an issue with wargaming overall, and just requires acceptance that wargames will not be able to replicate the same emotional pressure.

Problem: Information suspicion cannot be replicated.

There is the same issue with instilling suspicion of information in cyber wargames. At the Naval College, there are game nets where communication channels exist during war games. However, these game nets mainly exist to transmit, display and collect information as a mechanic of communication rather than a representation of specific real-world networks. The question is, how can designers introduce the idea that a network is compromised and make players wary of talking on that channel, or make players distrust a verification that the network is re-secured.[381] Marrin, Vogt, and Pellegrino note that the information aspect is particularly tricky because players are in a “pseudo-Truman” show, where the only information players receive is the information designers and adjudicators provide. [382]

[380] Marrin, Vogt, and Pellegrino.
[381] Marrin, Vogt, and Pellegrino.
[382] Marrin, Vogt, and Pellegrino.

Potential Solution: Game instructions or in-game injects can specify that information through digital channels could be compromised, and the follow-up with players at the end should point out areas of information manipulation or compromise.

Problem: Arbitrary Finite Operations

One of the challenges that CNA has encountered in wargaming cyber operations is the tendency of game designers to assign players a pre-set number of cyber effects. Often this is not related to a country's real capabilities in cyberspace. Pre-determined cyber tradecraft allocation can be the right choice for a wargame under certain circumstances—such as when available cyber tradecraft is already established, and players have the right level of access to discuss it. More often, designing a game with a pre-set number of cyber tradecraft includes cyber operations without fully integrating them into game play.[383]

Potential Solution: Some wargames will try to address this issue via resource allocation for different countries or entities, but, ultimately, it is a time-saving measure for gameplay.

Problem: Data Capture

While the difficulty of data capture is not a concern specific to cyber wargames, cyber operations and considerations do add another dimension to data analysis.

> "A good wargame includes a lot of people having a lot of conversation. From an analysis perspective, all of those conversations are data. You're trying to understand what people know and aggregate all that data. Even in an unclassified

[383] This problem was presented by Kate Lea during an interview.

environment when you can record information, it's hard to mike up everyone and have an individual transcription record. If people are willing to be miked up in the first place. Then, transcribe and have access to it, and then you have a volume of information problem that are transcribed verbatim into useful and actionable analysis."[384]

Potential Solution: Games that are run over digital channels can automatically capture player discussion, but data analysis will still rely on wargamer expertise and individual judgment.

While online board games do not have the same player interaction as virtual ones, they do allow for greater tracking of data and player communications. The SIGNAL game's online design gives it the advantage of "scalable data collection – expanding the wargaming participant pool from perhaps a dozen individuals in the traditional seminar-based format to thousands of online gamers."[385]

Recommendations: Cyber Wargaming as a Discipline

Talent Development is Key

Building a highly accurate, comprehensive, analytical wargame, requires both technical experts and wargame design experts. Ideally, leading the team would be a cyber wargaming expert, the same way that there are experts in nuclear wargames. Unfortunately, the field is very small, albeit growing. Most leading talent in the cyber wargaming field still is considered experts in wargaming first, who have then responded to a need for cyber wargames. This speaks to a larger problem within the wargaming and

[384] Sepinsky, Interview with Jeremy Sepinsky.
[385] Goldblum, Reddie, and Reinhardt, "Wargames as Experiments."

technical-policy community, where there is limited public awareness, and career options, for wargaming, and there is a divide in specialization between 'technical' cyber experts and 'policy' cyber experts. This means that, while there may be a desire to build more wargames or to have more 'technical' expert adjudication for higher realism, there also may simply be a lack of available talent or what experts are available are already committed. Wargaming as a career field is already a selective process with no talent pipeline or clear career path, and cyber wargaming is even more so.[386] If the United States wants to build better cyber wargames, it needs more cyber wargamers.

Running More Games with Different Formats

In addition to the aforementioned different ways of iterating games, cyber wargames can also attempt to combine the technical fidelity and the strategic effects through *multi-layered games.* Based on the games analyzed, there appears to be a divide between the highly technical and the effects-based response games. The former appears primarily in educational games, and the latter in analytical games. With a greater investment of resources, designers and sponsors could run multi-layered games that run both a tactical level and an operational or strategic level simultaneously, like Locked Shields but with the live-fire replaced with technical cyber experts discussing the known and unknown adversary systems.[387] While decision-makers game out a scenario, each move that makes is taken to a team of cyber experts that argue amongst themselves whether the attack would succeed, write down their reasoning for why or why not, and

[386] Bae, Interview with Sebastian Bae.
[387] "Locked Shields," accessed April 25, 2022, https://ccdcoe.org/exercises/locked-shields/.

send the information back to the decision-makers who can modify their request. The more games there are that try to combine cyber and non-cyber expert communication or encompass multiple layers of combat, the more holistic understanding decision-makers can access regarding cyberspace.

Rigorous, Complete Reports and Sharing Data in a Public Repository

For cyber wargaming to develop as a rigorous, academic methodology, we need published games and results. The DOD has a repository of classified wargames, but in interviews with experts, the general sentiment is that the database is far less utilized than desired.[388] The process for publishing reports into the database is a hassle, there is no standardization for what is put in the database (results, methods, background, instructions, adjudication decisions, etc.), and the database is rarely utilized by designers when building their wargames.[389] Designers often rely on their network inside their organization; the easiest thing to do is to phone up a colleague, rather than visit the database. However, this leaves a vast amount of previous wargaming knowledge unutilized.

In "The Handbook of Cyber Wargames," Curry and Drage note a list of ten important cyber wargames that have "varying amounts of detail, but little actual analysis of the outcomes and almost no discussion of the game mechanics used for the game."[390]

---

[388] Bartels, Interview with Elizabeth Bartel.
[389] Bartels.
[390] The list of games are, as follows: Deloitte Cyber Wargame, Department Homeland Security Control Systems Program, EU Summit March 2014, Locked Shields, Lockhead Martin US National Cyber Range Project, McKinsey & Company Standard model, Optimal Risks Company Standard Wargame model, Quantum Dawn 2 (Wall Street), Track 1.5, and Waking Shark II, listed in Curry and Drage, *The Handbook of Cyber Wargames: Wargaming the 21st Century*, 2.

That being said, how useful would a repository would actually be for wargaming experts is doubtful.[391] As a tool for budding designers, they may find value in looking at gaming mechanisms or how previous games have been built in the past. However, game design reports would need, to be useful to a designer building another game, to include insights as to the design process, specific mechanisms and game capabilities, and the thought process behind the structure to analysis – all of which is not typically included to game reports because it is not relevant to the sponsor.[392] Because of the specificity of games in answering a certain question at a certain time, it is easier to build a new game than to try to rely on previous simulations.[393]

A criticism of many of the analytical wargames listed is a lack of report information regarding participant demographics, game design, cyber capabilities, data collected, and future recommendations. By only presenting an analysis rather than the data gathered, it is difficult to verify, cross-check, or even draw separate conclusions regarding the implementation of the wargame and the gathered data. For instance, in Defend Forward, there is no data on what actions the Red or Blue State took under a "mutual vulnerability" strategy, no specific play-by-play of how the White Cell choose to interact and adjudicate with either group even though the game was unclassified and guidelines for cyber operations were explicitly based on open-source research and highly-abstracted. Just like any other science experiment in any other field, the need for

---

[391] It would be useful for this thesis, where tracking down cyber games with publicly accessible reports and resources has proved difficult. However, the author is also not a wargaming expert, having only designed one game for a 'sponsor' in an internship capacity, and therefore primarily has relied on other material rather than their own expertise or expertise within a parent organization.
[392] Interview with Unnamed Source.
[393] Interview with Unnamed Source.

transparent data is necessary for the reader to analyze the validity of the analysis.[394] While it is entirely possible that there was an internal report for "Lessons Learned," the concern lies not just with the individual game designers or the organization having recommendations to work off for the next game design, but the need for each separate organization or designer to 'start from scratch' each time a new game is built without a consolidated public database.

There is also no replicability when reports are sparse. When publishing an experiment in an academic journal, there are standards of replicability and verification that are expected: accurate methodology, procedure, data, and results analysis. However, analytical wargaming reports do not share the same standards. This is likely due to sponsor needs; the sponsor does not require a full-blown report, it is only concerned about the results. However, if wargaming wants to develop as a rigorous discipline, it needs more comprehensive reports so results can be replicated and peer-reviewed.

The concern for specifics when it comes to national security measures is always a balance between classified and unclassified information, however, if wargaming is to be useful, information must be public and be shared to a certain degree. The answer here may be relatively simple, write an unclassified report for academic publication and a classified report for those with the necessary security clearance. However, this still gets into the issue of whether or not these classified papers are being read and peer-reviewed by the necessary people – ultimately, as cyber wargames currently stand, we are trusting in the expertise of leading experts in their field to adequately and accurately analyze the

[394] Altuğ Tuncel and Ali Atan, "How to Clearly Articulate Results and Construct Tables and Figures in a Scientific Paper?," *Turkish Journal of Urology* 39, no. Suppl 1 (September 2013): 16–19, https://doi.org/10.5152/tud.2013.048.

results of a wargame. For example, Defend Forward 2019 mentions that research and analysis in combination with data of the two previous NWC critical infrastructure games will be useful moving forward, but these data sets are not publicly available.[395] If cyber wargaming is to be respected as a valuable educational and analytical tool, then it needs to prove its worth with first-hand public and peer access through better reports and data sharing.

[395] Cyber and Innovation Policy Institute Staff, "Defend Forward: Critical Infrastructure War Game 2019 Game Report," 8.

Conclusion

The United States is facing digital threats as adversarial groups are increasingly bold and creative in their use of cyber warfare. Cyber capabilities and cyber warfare pose a high barrier to comprehension: they are covert and hidden behind classification levels, involve highly technical methods, do not have their existence or probability of success verified, and are constantly updating and becoming obsolete. Cyber wargaming offers a method of conceptualizing and understanding cyber conflict in preparation for decision-making by representing cyber capabilities in abstracted forms, but this poses its own challenges of educational and analytical value.

The thesis creates a definition of cyber wargames based on its components, and applies this framework to over twenty wargames, supplemented by expert interviews. An analysis of the purpose and cyber representation in these games showcases different models of cyber wargames, each with its own drawbacks and limitations, with particular note of the design process behind Influence 2040. Based on this examination, the paper concludes by addressing the issues of cyber wargames and steps needed for the future where cyber wargaming becomes a rigorous, verified form of education and analysis.

Works Cited

Alperovitch, Dmitri. "One Reason Why We Are Not Seeing Much Cyber Activity in Ukraine Right Now: Cyber Is a Perfect Weapon for Grey Zone Conflict: The Space between Peace and War. Once War Breaks out, Cyber Becomes Much Less Useful for Anything but Very Tactical Objectives in Support of Kinetic Ops." Twitter, March 2, 2022. https://twitter.com/dalperovitch/status/1499136582770733061?s=21.

Arquilla, Jon. "The Rise of Strategic Cyberwar?" *Communications of the ACM* (blog), September 25, 2017. https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext.

BoardGame Geek. "Axis & Allies | Board Game | BoardGameGeek." Accessed April 4, 2022. https://boardgamegeek.com/boardgame/98/axis-allies.

Bae, Sebastian. Interview with Sebastian Bae, April 22, 2022.

———. "Littoral Commander." Dietz Foundation, 2022.

Banks, David. "War Games Shed Light on Real-World Strategies." The Conversation, April 19, 2019. http://theconversation.com/war-games-shed-light-on-real-world-strategies-113631.

Bartels, Elizabeth. "Building Better Games for National Security Policy Analysis." Dissertation. RAND Institute, March 2020.

———. "Getting the Most Out of Your Wargame: Practical Advice for Decision-Makers," November 19, 2019. https://warontherocks.com/2019/11/getting-the-most-out-of-your-wargame-practical-advice-for-decision-makers/.

———. "Incorporating Gaming into Research Programs in International Relations: Repetition and Multi-Method Analysis." ISA Annual Conference, April 8, 2020. http://www.elliebartels.com/uploads/1/1/0/6/110629149/bartels_multi_method_games_8april2021.pdf.

———. "Innovative Education: Gaming - Learning at Play." *ORMS Today* 41, no. 4 (August 2014). https://pubsonline.informs.org/do/10.1287/orms.2014.04.13/full/.

———. Interview with Elizabeth Bartel, November 23, 2022.

Bartos, Christopher. "Cyber Weapons Are Not Created Equal." *Proceedings* 142, no. 6 (June 1, 2016). https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal.

Beury-Russo, Lisa. Takeaways from the Cyber Storm exercise, August 23, 2020. https://govmatters.tv/takeaways-from-the-cyber-storm-exercise/.

Bose, Nandita. “Biden: If U.S. Has ‘real Shooting War’ It Could Be Result of Cyber Attacks.” *Reuters*, July 28, 2021, sec. World. https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/.

Brantly, Aaron F. “The Cyber Deterrence Problem.” In *2018 10th International Conference on Cyber Conflict (CyCon)*, 31–54. Tallinn: IEEE, 2018. https://doi.org/10.23919/CYCON.2018.8405009.

Brown, Joseph M., and Tanisha M. Fazal. “#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations.” *European Journal of International Security* 6, no. 4 (November 2021): 401–17. https://doi.org/10.1017/eis.2021.18.

Carroll, Patrick. “Strategic, Operational, and Tactical Wargames | Solitary Soundings.” *BoardGameGeek* (blog), June 12, 2011. https://boardgamegeek.com/blogpost/2919/strategic-operational-and-tactical-wargames.

Cattler, David, and Daniel Black. “The Myth of the Missing Cyberwar,” April 13, 2022. https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.

Chen, Sarah, Chloe Hyman, Cyrus Jabbari, Daniel Brickhill, Fahad Mirza, Ian Harrison, John Ketterer, et al. “Influence 2040 Card Capabilities,” June 5, 2020.

———. “Influence 2040 Rulebook,” June 5, 2020.

CISA. “Cyber Games | CISA.” Accessed April 5, 2022. https://www.cisa.gov/cybergames.

———. “Cyber Storm 2020: After-Action Report.” Cybersecurity and Infrastructure Security Agency, August 2020.

———. “Cyber Storm: Securing Cyber Space | CISA.” Accessed April 14, 2022. https://www.cisa.gov/cyber-storm-securing-cyber-space.

———. “Cyber Storm VIII: National Cyber Exercise,” March 2022. https://www.cisa.gov/cyber-storm-viii-national-cyber-exercise.

———. “Official Alerts & Statements - CISA | CISA,” 2022. https://www.cisa.gov/stopransomware/official-alerts-statements-cisa.

CNA. “So You Want to Sponsor a Wargame...” Center for Naval Analyses, n.d. https://www.cna.org/centers/cna/operational-warfighting/wargaming.

———. “Wargaming | CNA.” Accessed November 30, 2021. https://www.cna.org/centers/cna/operational-warfighting/wargaming.

“CONTRACT to BOOZ ALLEN HAMILTON INC. | USAspending.” Accessed November 17, 2021. https://usaspending.gov/award/CONT_AWD_70RCSA20FR0000085_7001_GS00Q14OADU108_4732.

Copp, Tara. “‘It Failed Miserably’: After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight.” Defense One, July 26, 2021. https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/.

Curry, John. Interview with John Curry, February 2, 2022.

Curry, John, and Nick Drage. *The Handbook of Cyber Wargames: Wargaming the 21st Century*, 2020.

Curry, John, and Tim Price. *Dark Guest Training Games for Cyber Warfare*, 2013.

Cyber and Innovation Policy Institute Staff. “Defend Forward: Critical Infrastructure War Game 2019 Game Report.” Cyber and Innovation Policy Institute, 2019. https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Cyber%20&%20Innovation%20Policy%20Institute/Defend%20Forward%20Critical%20Infrastructure%20Game%20Report%202019.pdf?sr=b&si=DNNFileManagerPolicy&sig=%2Bdh86X6w60GJ4B6iTHCbiq3T8iOQ8Oy0PIIlZiCbzUM%3D.

Davis, Sally. “Review: We Come In Peace, a Game about Cultural Misunderstanding.” *PAXsims* (blog), December 12, 2020.

Department of Homeland Security. “Draft National Cyber Incident Response Plan.” Department of Homeland Security, September 2010. https://www.cisa.gov/uscert/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf.

———. “Draft National Cyber Incident Response Plan.” Department of Homeland Security, September 30, 2016. https://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf.

———. “National Cyber Incident Response Plan.” Department of Homeland Security, December 2016. https://www.cisa.gov/uscert/ncirp.

———. “National Response Plan Brochure,” n.d. https://www.dhs.gov/xlibrary/assets/NRP_Brochure.pdf.

DeYoung, Greg Jaffe and Karen. “U.S. Tested 2 Afghan Scenarios in War Game,” October 26, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/10/25/AR2009102502633.html.

Dix Jr, Robert. “A National Cyber Event Requires Clarity for Roles and Responsibilities.” SIGNAL Magazine, May 28, 2015. https://www.afcea.org/content/Blog-national-cyber-event-requires-clarity-roles-and-responsibilities.

Dstl. “Cyber Card Game.” Dstl, n.d. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043232/Easy_Access_IP_Cyber_Card_Game.pdf.

Eikmeier, Dale. “Waffles or Pancakes? Operational- versus Tactical-Level Wargaming.” *Joint Force Quarterly*, July 2015. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/607625/waffles-or-pancakes-operational-versus-tactical-level-wargaming/.

Ferran, Lee. “Russian Hackers Raided Defense Contractors for Two Years, Stole Sensitive Info: US.” *Breaking Defense* (blog), February 16, 2022. https://breakingdefense.sites.breakingmedia.com/2022/02/russian-hackers-raided-defense-contractors-for-two-years-stole-sensitive-info/.

Fischerkeller, Michael, and Richard Harknett. “What Is Agreed Competition in Cyberspace?” Lawfare, February 19, 2019. https://www.lawfareblog.com/what-agreed-competition-cyberspace.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (2013): 41–73.

Gill, Jaspreet. “Pentagon Wants $11.2B for Cyberspace Security, Training in FY23.” *Breaking Defense* (blog), March 30, 2022. https://breakingdefense.sites.breakingmedia.com/2022/03/pentagon-wants-11-2b-for-cyberspace-security-training-in-fy23/.

Glover, Claudia. “New Malware Could Allow ‘low-Skill’ Hackers to Disrupt Critical Infrastructure.” *Tech Monitor* (blog), April 14, 2022. https://techmonitor.ai/technology/cybersecurity/incontroller-malware-critical-national-infrastructure.

Goldblum, Bethany, Andrew Reddie, and Jason Reinhardt. “Wargames as Experiments: The Project on Nuclear Gaming’s SIGNAL Framework.” *Bulletin of the Atomic Scientists* (blog), May 29, 2019. https://thebulletin.org/2019/05/wargames-as-experiments-the-project-on-nuclear-gamings-signal-framework/.

Goldman, David. “Shodan: The Scariest Search Engine on the Internet.” CNNMoney, April 8, 2013. https://money.cnn.com/2013/04/08/technology/security/shodan/index.html.

Gondree, Mark. *TableTopSecurity/D0x3d-the-Game*. TeX. 2012. Reprint, TableTopSecurity, 2022. https://github.com/TableTopSecurity/d0x3d-the-game/blob/a4ea2e01cf631770c1c28290f024a75c56d6fbe1/instructions/d0x3d-rules-v2.pdf.

Grant, Virginia. “Wargames.” *Los Alamos National Laboratory*, July 26, 2021. https://discover.lanl.gov/publications/national-security-science/2021-summer/wargames.

Haggman, Andreas. “Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education.” PhD Thesis, University of London, 2019.

Haggman, Andrew. Interview with Andrew Haggman, March 24, 2022.

Hall, Nic. “2d TSB Cybersecurity Division at the Forefront of the World’s Largest Live-Fire Cyber Exercise.” *U.S. Army*. August 14, 2018.

Harwell, Drew. “Instead of Consumer Software, Ukraine’s Tech Workers Build Apps of War.” *Washington Post*, March 24, 2022. https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/.

Healey, Jason, and Robert Jervis. “The Escalation Inversion and Other Oddities of Situational Cyber Stability.” *Texas National Security Review*, September 28, 2020. https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

Hopkins, Nick. “US and China Engage in Cyber War Games.” *The Guardian*, April 16, 2012. https://www.theguardian.com/technology/2012/apr/16/us-china-cyber-war-games.

Hunt, Edward. “US Government Computer Penetration Programs and the Implications for Cyberwar.” *IEEE Annals of the History of Computing* 34, no. 3 (July 2012): 4–21. https://doi.org/10.1109/MAHC.2011.82.

Interview with Unnamed Source, February 19, 2022.

Jackson, Steve. “Hacker: The Computer Crime Card Game.” Steve Jackson Games, 2001.

Joint Publication 5-0. “Joint Planning.” Washington, DC: The Joint Staff, December 1, 2020.

Judah, Tim. “How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders.” *Financial Times*, April 10, 2022. https://www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8.

Kick, Jason. “Cyber Exercise Playbook.” The MITRE Corporation, 2014.

KızBaşına Women in Command Project Team. GUWS x KizBasina: Hybrid Threats Rising Playthrough, February 19, 2022.

———. “Hybrid Threat Rising Wargame.” KizBasina, 2021.

Kollars, Nina, and Benjamin Schechter. “Pathologies of Obfuscation: Nobody Understands Cyber Operations or Wargaming.” *Atlantic Council*, February 1, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pathologies-of-obfuscation-nobody-understands-cyber-operations-or-wargaming/.

Kube, Courtney, and Ken Dilanian. “Biden given Options for Unprecedented Cyberattacks against Russia.” NBC News, February 24, 2022. https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.

Lea, Kate. Interview with Kate Lea, March 2, 2022.

Li, Yuchong, and Qinghui Liu. “A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments.” *Energy Reports* 7 (November 1, 2021): 8176–86. https://doi.org/10.1016/j.egyr.2021.08.126.

Libeskind-Hadas, Ran. Conversation with Professor Ran Libeskind-Hadas, November 16, 2021.

Libicki, Martin C. “Crisis and Escalation in Cyberspace,” January 3, 2013. https://www.rand.org/pubs/monographs/MG1215.html.

Lin-Greenberg, Erik. Interview with Erik Lin-Greenberg, March 11, 2022.

Lin-Greenberg, Erik, Reid B.C. Pauly, and Jacquelyn G. Schneider. “Wargaming for International Relations Research.” *European Journal of International Relations*, December 17, 2021, 13540661211064090. https://doi.org/10.1177/13540661211064090.

Linick, Michael E., John Yurchak, Michael Spirtas, Stephen Dalzell, Yuna Huh Wong, and Yvonne K. Crane. “Hedgemony: A Game of Strategic Choices.” RAND Corporation, September 21, 2020. https://www.rand.org/pubs/tools/TL301.html.

“Locked Shields.” Accessed April 25, 2022. https://ccdcoe.org/exercises/locked-shields/.

Longley-Brown, Graham. “What Is Wargaming? | LBS,” 2015. http://lbsconsultancy.co.uk/our-approach/what-is-it/.

Lubin, Randy. “Diegetic Games | CIA Collect It All,” 2016. https://diegeticgames.com/cia-collect-it-all/.

Luttwak, Edward N. “The Operational Level of War.” *International Security* 5, no. 3 (1980): 61–79. https://doi.org/10.2307/2538420.

Mandiant. “Targeted Attack Lifecycle | Mandiant,” 2022. https://www.mandiant.com/resources/targeted-attack-lifecycle.

Marrin, Don, Walter Berberick, and Wargaming Department. “Global Title X Series ’13: Game Report.” Game Reports. U.S. Naval War College, 2014. https://digital-commons.usnwc.edu/game-reports/13/.

———. “Global Title X Series ’14.” Game Reports. U.S. Naval War College, 2015. https://digital-commons.usnwc.edu/game-reports/15/.

Marrin, Don, Walter Berberick, Wargaming Department, and David Ward. “Global Title X Series ’10: Global Maritime Partnership Game.” Game Reports. U.S. Naval War College, 2010. https://digital-commons.usnwc.edu/game-reports/12.

Marrin, Don, Jason Vogt, and Peter Pellegrino. Interview with Don Marrin, Jason Vogt, and Peter Pellegrino, March 18, 2022.

Maschmeyer, Lennart. “Why Cyber War Is Subversive, and How That Limits Its Strategic Value.” War on the Rocks, November 17, 2021. https://warontherocks.com/2021/11/why-cyber-war-is-subversive-and-how-that-limits-its-strategic-value/.

Matherly, John. “State of Control Systems in the USA.” Shodan Blog, May 15, 2015. http://blog.shodan.io/state-of-control-systems-in-the-usa-2015-05/.

McCardle, Jennifer. Interview with Jennifer McCardle, December 6, 2021.

McGrady, Ed. “Building Speculative Games.” Representing Artificial Intelligence in Wargames. Connections 2020, December 2020.

———. “Getting the Story Right about Wargaming.” War on the Rocks, November 8, 2019. https://warontherocks.com/2019/11/getting-the-story-right-about-wargaming/.

———. Interview with Ed McGrady, February 18, 2022.

McHugh, Francis. “Appendix C - A Glossary of War Gaming Terms.” In *Fundamentals of War Gaming*, 3rd ed., 1966.

BoardGameGeek. “Men Under Fire.” Accessed April 5, 2022. https://boardgamegeek.com/boardgame/128490/men-under-fire.

Metcalf, Andrew, and Christopher Barber. “Tactical Cyber: How to Move Forward.” *Small Wars Journal*, September 14, 2014. https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward.

MITRE. “MITRE ATT&CK®,” 2021. https://attack.mitre.org/.

———. “Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle.” The MITRE Corporation, 2015. http://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf.

Mouat, Tom. “Cyber Card Game.” Wargame Session presented at the Georgetown Wargaming Society, Dtsl UK, February 13, 2022.

———. Interview with Major Tom Mouat. Online Interview, February 7, 2022.

MuckRock. “Materials for the Game ‘Collection Deck.’” MuckRock, March 18, 2017. https://www.muckrock.com/foi/united-states-of-america-10/materials-for-the-game-collection-deck-35175/.

National Cyber Security Division. “Cyber Storm Exercise Report.” Department of Homeland Security, September 12, 2006. https://www.cisa.gov/cyber-storm-i.

———. “Cyber Storm II Final Report.” Department of Homeland Security, 2008. https://www.cisa.gov/publication/cyber-storm-final-reports.

———. “Cyber Storm III Final Report.” Department of Homeland Security, July 2011. https://www.cisa.gov/publication/cyber-storm-final-reports.

———. “Cyber Storm V: After Action Report.” Department of Homeland Security, July 2016. https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

———. “Cyber Storm VI: After Action Report.” Department of Homeland Security, 2018. https://www.cisa.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

———. “Informing Cyber Storm V: Lessons Learned from Cyber Storm IV.” Department of Homeland Security, June 2015. https://www.cisa.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf.

Parson, Edward. “What Can You Learn from a Game?” In *Wise Choices: Games, Decisions,l and Negotations*, edited by R. Zeckhauser, R. Keeney, and J. Sevenius. Harvard Business School Press, 1966.

Paul, Kari. “‘Catastrophic’ Cyberwar between Ukraine and Russia Hasn’t Happened (yet), Experts Say.” *The Guardian*, March 9, 2022, sec. Technology. https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.

Pauly, Reid. Interview with Reid Pauly, February 16, 2022.

Perla, Peter. *The Art of Wargaming: A Guide for Professionals and Hobbyists*. Annapolis, MD: Naval Institute Press, 1990.

Perla, Peter P. “What Wargaming Is and Is Not.” *Naval War College Review* 38, no. 5 (1985): 70–78.

RAND. “Wargaming.” Accessed April 6, 2022. https://www.rand.org/topics/wargaming.html.

Rid, Thomas. “Why Hacking Is Way Too Easy.” The Sydney Morning Herald, July 31, 2013. https://www.smh.com.au/technology/why-hacking-is-way-too-easy-20130726-hv153.html.

Romaniuk, Scott. “Military Strategy and the Three Levels of Warfare.” Defense Report, November 30, 2017. https://doi.org/10.13140/RG.2.2.26287.79528.

Rovner, Joshua. “Cyber War as an Intelligence Contest.” War on the Rocks, September 16, 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

Sanger, David. “The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.” Wilson Center, 2018.

Sanger, David E., and Mark Mazzetti. “U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict.” *The New York Times*, February 16, 2016, sec. World. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Sanger, David E., and Emily Schmall. “China Appears to Warn India: Push Too Hard and the Lights Could Go Out.” *The New York Times*, February 28, 2021, sec. U.S. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

SAYIN, Elçin Ada. Interview with Elçin Ada SAYIN, April 13, 2022.

Schechter, Benjamin, Jacquelyn Schneider, and Rachael Shaffer. "Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming." *Simulation & Gaming* 52, no. 4 (August 1, 2021): 513–26. https://doi.org/10.1177/1046878120987581.

Schneider, Jacquelyn. "This Is Exactly What I Found in Wargames--Once Bombs Are Being Dropped, the Primary Role for Cyber Operations Comes in Supporting Conventional Operations . . . but This Is Tactically Very Difficult Because Networks Are Changing." Twitter, March 2, 2022. https://twitter.com/jackiegschneid/status/1499137881205403650?s=21.

Sepinsky, Jeremy. Interview with Jeremy Sepinsky, March 28, 2022.

Shandler, Ryan, Michael L. Gross, Sophia Backhaus, and Daphna Canetti. "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment." *British Journal of Political Science* 52, no. 2 (February 2021): 850–68. https://doi.org/10.1017/S0007123420000812.

Simpson Jr., William L. "A Compendium of Wargaming Terms." MORS, September 20, 2017. www.mors.org/communities/wargaming.

Smith, Frank. Interview with Frank Smith, March 9, 2022.

Steinzer, Chris. "We Should Never Say That a Wargame 'Proved' or 'Validated' Anything. Nor Should We Ever Expect Games to Be Predictive." Twitter, April 5, 2022. https://twitter.com/SteinitzChris/status/1511340161002610697.

Trevithick, Joseph. "The U.S. Army Invented Five Fake Countries." *War Is Boring* (blog), June 16, 2016. https://medium.com/war-is-boring/the-u-s-army-invented-five-fake-countries-58dcc7dad790.

Trofimov, Yaroslav. "A Ukrainian Town Deals Russia One of the War's Most Decisive Routs." *WSJ*, March 16, 2022, sec. World. https://www.wsj.com/articles/ukraine-russia-voznesensk-town-battle-11647444734.

Tuncel, Altuğ, and Ali Atan. "How to Clearly Articulate Results and Construct Tables and Figures in a Scientific Paper?" *Turkish Journal of Urology* 39, no. Suppl 1 (September 2013): 16–19. https://doi.org/10.5152/tud.2013.048.

BoardGameGeek. "Twilight Imperium: Fourth Edition." Accessed April 5, 2022. https://boardgamegeek.com/boardgame/233078/twilight-imperium-fourth-edition.

BoardGame Geek. "Twilight Struggle | Board Game | BoardGameGeek." Accessed April 4, 2022. https://boardgamegeek.com/boardgame/12333/twilight-struggle.

U.S. Army. "Decisive Action Training Environment." TRADOC G-2. Ft. Leavenworth, Kansas: U.S. Army, April 2015.

———. “Threat Tactics Report: Syria.” TRADOC G-2 ACE Threats Integration, February 2016.

U.S. Government. “Cyber Incident Annex National Response Plan.” U.S. Government, 2004. https://www.hsdl.org/?view&did=484571.

Us Naval War College. “About Wargaming.” Accessed March 9, 2022. https://usnwc.edu/Research-and-Wargaming/Wargaming/About-Wargaming.

USAF College of Aerospace Doctrine, Research and Education. “Three Levels of War.” In *Air and SPace Power Mentoring Guide*, Vol. 1. Maxwell AFB: Air University Press, 1997.

Valeriano, Brandon. Interview with Brandon Valeriano, April 22, 2022.

Vergun, David. “‘Persistent Engagement’ Strategy Paying Dividends, Cybercom General Says > U.S. Department of Defense > Defense Department News.” U.S. Department of Defense, November 10, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2840284/persistent-engagement-strategy-paying-dividends-cybercom-general-says/.

Visky, G. “Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations,” 2020. https://www.semanticscholar.org/paper/Cyber-in-War%3A-Assessing-the-Strategic%2C-Tactical%2C-of-Visky/fdf5e3f147b8447f699d5b60c8da4e3c78b94e4a.

Connections Wargaming Conference. “Wargaming,” June 2, 2015. https://connections-wargaming.com/wargaming/.

Welburn, Jonathan William, Justin Grana, and Karen Schwindt. “Cyber Deterrence or: How We Learned to Stop Worrying and Love the Signal,” September 4, 2019. https://www.rand.org/pubs/working_papers/WR1294.html.

Wickström, G., and T. Bendix. “The ‘Hawthorne Effect’--What Did the Original Hawthorne Studies Actually Show?” *Scandinavian Journal of Work, Environment & Health* 26, no. 4 (August 2000): 363–67.

Wolcott, Harry, Sarah Baker, and Rosalind Edwards. “Introduction.” In *How Many Qualitative Interview Is Enough? Expert Voice and Early Career REflections on Sampling and Cases in Qualitative Research*, 4. National Centre of Research Methods, 2012.

Wong, Yuna. Interview with Yuna Wong, February 19, 2022.

Wong, Yuna, Elizabeth Bartels, Benjamin Smith, and Sebastian Bae. “Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action.” Santa Monica, CA: RAND, 2019.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group, 2014.