Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Pathologies of Obfuscation:
Nobody Understands Cyber Operations or Wargaming

FEBRUARY 2021 NINA KOLLARS AND BENJAMIN SCHECHTER

Executive Summary
National security and defense professionals have long utilized wargames to better understand hypothetical conflict scenarios. With conflict in the cyber domain becoming a more prominent piece in wargames in the national security community, this issue brief seeks to identify the common pathologies, or potential pitfalls, of cyber wargaming. It argues that the inherent turbulence of the cyber domain and segmented knowledge about cyber weapons negatively affect three components of cyber wargaming: the scenario development, the data usability, and the cross-participant comprehensibility. The brief offers some initial solutions to these problems, but, ultimately, the purpose of identifying pathologies is to prepare designers to meet these challenges in each unique design.

Introduction
Wargaming is seeing a resurgence in popularity among future warfighting thinkers. This is doubly so with respect to its cyber form. Wargaming places human players into complex and uncertain environments, and asks them to make choices in a steadily unfolding scenario of the designer's choosing. For veteran wargame designers, managing the game toward its desired end state is a matter of balancing art and science. This is particularly because wargame designers are not omnipotent, they rely upon the cooperative spirit of experts across the broad range of military and civilian practitioners. Every person participating in and facilitating the game controls a piece of the game's outcome.

The problem is that both cyberspace and wargaming are fraught with technical and infrastructural perplexities. Experts in cyberspace are often not experts in wargaming, and vice versa. Moreover, players, observers, and report readers frequently don't understand the specifics of cyber or wargaming very well. Thus, bringing the two together complicates both.

For wargamers brave enough to tackle it, cyber wargaming can be remarkably rewarding as a study in decision-making at tactical, operational, and strategic levels, but it is no easy path. Wargames, whether for research or education, can be a powerful tool for discovery and exploration of human decision-making. The cyber domain provides new challenges, but also tantalizing research questions. Wargames allow practitioners to peer into

hypothetical instances of conflict, allowing them to think through fighting without conflict on a real-world battlefield.

Wargaming is subject to myriad categorizations and classifications, but there is one relatively common, and compelling, typology. Nearly fifteen years ago, some of the foremost experts in wargaming came together and penned a document about wargame failure evocatively titled "Wargame Pathologies."[1] The resulting report identifies the pathologies of unhealthy wargames. In other words, it explores the characteristics of wargames that cause them to defeat or fail to meet the wargame designer's objectives. The authors provide a key organizing frame for future game designers, regardless of the game's emphasis or scope. The authors' purpose here is to connect their structured notion of wargame pathologies to cyber-specific wargaming.[2] They ask: What characteristics or factors of the cyber domain are likely to result in pathological outcomes in wargaming?

"Wargame Pathologies" laid out the essential elements of a wargame—the objectives, scenario, database, models, rules, infrastructure, participants, analysis, culture, and audience—and systematically reasoned how weaknesses in each could drive a game to failure. The authors, combining expertise from CNA and the Naval War College, add to this their initial analysis of the cyber domain, as well as the complex interplay of software, hardware, networks, users, and organizations. Their reflections on unhealthy cyber wargames are but a small part of a much larger project currently in progress at the Naval War College. Over the last year, the scholars of the Cyber and Innovation Policy Institute (CIPI) have conducted targeted outreach to professional military education (PME) institutions, cybersecurity firms, think tanks, and globally recognized wargamers to assess the state of the art in cyber wargaming.

The intent here is to reflect on some of the authors' initial struggles with unhealthy cyber-wargame pathologies and to help others avoid similar problems. A more extensive treatment of their work will be published later this year in a cyber-wargaming compendium.[3] Thus far, they have identified two preliminary characteristics of cyberspace and cyber tools—their turbulent character and segmented knowledge—that can create uncertainty in three game elements—participants, databases, and scenarios. As Christopher Weuve and his co-authors know, instability in game elements drives failure. Here the authors discuss these characteristics and their impact on game elements, and conclude with some thoughts about moving forward.

Confounding Characteristics of Cyber

Two elements of cyberspace—the environment and cyber tools—are particularly important to wargames and wargame designers. However, the cyber domain's dynamically shifting dependencies and the highly segmented and diffuse knowledge about cyber tools (and their effects) mean designing the cyber environment, cyber tools, and modeling the effects of those tools on the environment are persistent challenges and potential sources of cyber-wargame pathologies.

Dynamic Technologies, Turbulent Environment

All wargames contain abstractions. No game is designed to capture all the minutiae of land, air, sea, or space. Instead, these domains are represented through abstractions or simplifications, providing just enough detail for players to understand and act within the game world. For instance, the undersea environment has varying degrees of depth, temperature, density, etc. A wargame designer selects from known and relevant aspects of this environment to depict the domain. Much of the labor of "filling in the blanks" is then left to the participants' knowledge and experience. These representations of physical domains are, at least in theory, comprehensible and sharable through participants' personal experience.

With cyber, there is little tacit agreement among operators, technologists, and scholars about the terrain, including its scope, the technologies involved, and the socio-technical dependencies between those machines and human users. Some of these dependencies are touted as enablers of cyber warfare in JP 3-12, the Joint Publication for Cyberspace Operations.[4] It is one thing to know that computing systems are connected, however, and another thing entirely to meaningfully abstract them.

1 Christopher A. Weuve, et al., "Wargame Pathologies," Naval War College, September 2004, https://www.cna.org/CNA_files/PDF/D0010866.A1.pdf.

2 Ibid.; Benjamin Schechter, "Wargaming Cyber Security," *War on the Rocks, September 4, 2020, https://warontherocks.com/2020/09/wargaming-cyber-security/.*

3 For more information on the release date and publisher for the compendium, please contact Cyber and Innovation Policy Institute Director Dr. Frank Smith.

4 "Cyberspace Operations," Joint Chiefs of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

There is a constant churn in the hardware and software that make up the Internet, not to mention the millions upon millions of new Internet of Things (IoT) devices, phones, and systems connected to the Internet daily.[5] If that were all, a wargame might be able to capture it well; however it isn't only the machines in play. Perhaps more importantly, human behavior is present amidst this technical context. Human (in)comprehension of technological churn—the constant updating, upgrading, replacing, reformatting, repurposing, and modifying—can create new vulnerabilities and new kinds of attack, spilling over into entirely different geographic areas, legal regimes, and organizational spaces. That spillover generates the need for new kinds of responses, laws, organizations, and, in turn, new kinds of hardware and software.

It is difficult to understate the confounding nature of this problem for cyber wargames. In most games set in other domains, the behavior of that domain (air, sea, land, space) is well understood. There is scant need, for instance, in a Pacific Ocean scenario to begin with, "assume the ocean works roughly the same throughout the entire game, and exactly as it worked last time."

Yet, in a cyber wargame, the terrain can plausibly shift or disappear entirely over the course of the game. This is akin to declaring that the ocean might be ice for the next three hours but then dry up entirely for twenty minutes, or that ships moving on the water's surface will inexplicably sink or teleport to the other side of the Earth. This is perhaps an overstatement, but it brings this discussion closer to understanding the difficulty in arriving at enduring and mutually comprehensible abstractions of cyberspace. The churn in this domain means that designers of iterated games played annually or with longer gaps often struggle to credibly represent cyberspace for their players.

By way of example, during the two iterations of the Naval War College's Critical Infrastructure wargame (the first of which was run in 2017, and the second in 2019), the relevant software and technology used in each sector changed—and so did the protocols, information-sharing regimes, and organizations. The financial-services sector, for example, was noteworthy for its rapid adaptation to cloud computing in less than two years. The perceived trend may have been real or simply a passing moment, but it highlights the rapidity and depth of change. The wargames also incorporated multiple critical-infrastructure sectors, and each had markedly different rates and types of change. The highly interconnected nature of critical infrastructure meant that changes in one sector had consequences across the entire domain. Intentional system changes can have cascading effects just as consequential as any cyberattack.

Creating standardized templates for cyberspace operations, or even static networks, is then complicated by the rapid rate of change to the system. Models and databases accounting for specific operations and network or system properties are quickly overcome by events or become outdated. The changes are not trivial; the uptake of software as a service, infrastructure as a service, and other "as service" products attest to how rapidly conditions change.

Knowledge of Cyber Weapons and Their Effects is Segmented and Diffuse

The second characteristic of the current cyber environment is segmented and diffuse knowledge about cyber tools, implantation, and their effectiveness. Unlike many nuclear weapons, or conventional military platforms, authoritative data about cyber threats, attacks, capabilities, and their effects are distributed across varying state actors, private-sector firms, and white-, grey-, and black-hat hacking collectives. Distributed data about cyber tools and effects mean that there are no currently agreed-upon means to represent offensive weapons or defensive responses, or to quantify their effects on the cyber environment. To be clear, there are data, but the data are collected and held separately. Private-sector cybersecurity firms capture and hold very fine-grained data that are derived directly from the clients they protect. Meanwhile, Department of Defense data are both segmented and highly classified in individual special-access programs.

Certainly, not all such data are stovepiped; some sharing of tools and their effects does occur. Private-sector firms sometimes share threat data across their sectors to defend collectively via what are known as ISACs (information-sharing and analysis centers). Certainly, the entire MITRE ATT&CK knowledge base of tactics and techniques is used in a number of highly tactical cyber games at the corporate or lower levels to inform

5 Fredrik Dahlqvist, et al., "Growing Opportunities in the Internet of Things," McKinsey, July 2019, https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things.

response programs, or to discover gaps in corporate defenses.[6] Offensively, however, data are scant. Some of the information even reaches government entities or flows across sectors. But, there are simultaneous incentives for companies, cybersecurity firms, and individuals to keep knowledge to themselves to monetize it on black, grey, and white markets.[7]

There is little natural harmony of interests for firms and governments to create unified manuals covering effects, tools, and offensive platforms for wargamers and planners. Knowledge is power in cyberspace and, therefore, is hard to come by in cyber wargaming. The lack of harmony is not unique to cyber, however. Take, for instance, medicine and public health. There are government agencies like the National Institutes for Health and the Centers for Disease Control, hospitals and healthcare practitioners that treat individuals, and of course, the biomedical industry that produces medical therapies. They all work on health, but each holds specialized information—pharma companies hold specialized proprietary knowledge, hospitals have usage and outcome data, federal agencies collect national-level data. They all exist in the same space, each holding some of the data and processes. Collectively, they may have clarity on a range of health issues, but they are not exactly harmonious. Cyber also contains this broad spectrum of interests, data, and competition. The result leaves wargames designers—as well as many cyber practitioners—with an incomplete, muddled, and sometimes-conflicting view of cyber tools and their effects. And, this all assumes that there hasn't been a new patch released somewhere that hinders some cyber tools and enables others.

Thus, while in conventional Department of Defense wargames there are generally agreed-upon baseline measures of the contemporary weapons of war, cyber experts do not yet have reliable aggregation of data that they agree is the standard. Instead, they appear to be continually recreating the wheel when it comes to cyber effects.

Pathologies in Scenarios, Data, and Participants

Domain turbulence and segmented knowledge about weapons and their effects directly affect three components of cyber wargaming—the scenarios, the data, and the participants.

Game scenarios are the setting, the situational frame in which players are expected to interact and make decisions. They have a beginning state—including the initial conditions and "level of war" for the wargame—and an end state—objectives, win/lose conditions, and a point of termination. Between those two states, the scenario helps establish expected player actions and activities, available resources, and their command relationship—their place in the hierarchy of decision—as connects to other players and other game elements.[8] Typically, the scenario works as part of the orientation and motivation for the players to make their moves. But, where does it stop, and how up to date does the system's representation need to be?

The scenario is the first exposure the participants will have in experiencing what or how cyberspace is represented in the game. This is no small task. Scoping cyberspace is one of the most fundamental dilemmas in cyber-wargaming design. A realistic representation of the domain and all of its arbitrary dependencies, associated laws, organizations, and technologies is a nearly impossible task.

Scoping a dynamic domain risks accidentally trimming out emerging real-world phenomena that could fundamentally alter gameplay. Poor specification of what cyber is in a scenario can also lead to bias regarding expectations of what the domain is for (warfighting, criminal activities, information influence, etc.), which can then stifle cyber play if the proposed play space is ill-defined. Similarly, the scenario can overemphasize cyber as the one and only domain in which action takes place, which can also skew play.

Solutions? Not all is lost. At the national or strategic level, it appears organizations and legal regimes are stabilizing around continued technological change. At least at the highest echelons, there is a generally agreed-upon cast of characters, such as the telecommunications networks,

6 David B. Fox, et al., "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," MITRE, November 2018, https://www.mitre.org/publications/technical-papers/cyber-wargaming-framework-for-enhancing-cyber-wargaming-with-realistic.

7 "A Global Black Market for Stolen Personal Data," Trend Micro, https://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/.

8 Weuve, et al., "Wargame Pathologies," 16.

major technology firms, the banking sector, US Cyber Command, the Department of Energy, the Department of Homeland Security, and the National Security Agency. For the time being, it may mean that games are potentially on safer ground when remaining constrained to a narrow set of agencies, depending on the cyber objectives, interactions, or insights sought from a game, instead of attempting to chase the most realistic scenario.

In games at the operational or tactical level—the level of a city or transnational corporation—the solutions are less clear cut. In developing believable scenarios and abstractions for cyberspace, laying clear expectations of the purpose of the abstraction, and being transparent in the underlying assumptions can help. Then players at least have a common, albeit imperfect, understanding and allow the game to proceed.

Game databases for cyber are, in the authors' experience, one of the largest roadblocks, particularly for research and analytic cyber wargames. Unfortunately, there is no single agreed-upon set of cyber tools or their effects; cyberspace is too turbulent and the existing data too disbursed to develop reliable statistics. Databases are the quantitative weights and measures within a game. A game database will, for example, include every weapon, platform, system, and sailor in the game to the level of detail appropriate (a strategic-level game doesn't need to name every sailor). This includes any relevant information on how those things operate within the game (for example, missile ranges and hit probabilities). These quantitative weights and measures feed directly into the cyber tools and effects expressed during gameplay.[9] Wargamers just can't predict the effects of a piece of malware the same way they can with a cruise missile. This grim reality makes any game database instantly suspect, not to be believed or trusted, and can tilt the game into a failure mode.[10] Much like how scoping the cyber environment can produce biased play or beliefs about how cyber works, so can the mismeasurement of cyber effects produce knock-on effects, leading to too much or too little confidence in cyber play.

Solutions? It is unlikely that there will be a unified cyber tools and effects database anytime soon. Instead, the authors have observed that most game designers build workarounds through careful design, or rely heavily on their cyber experts.

One way forward is to focus less upon the specific quantitative realism of, for instance, a piece of weaponized malware, and instead proceed openly in dialogue with cyber adjudicators working directly with players as the game progresses. Even this has its limitations, however. The excessive segmentation of knowledge among cyber experts means that either the white cell is brimming with experts who may ultimately go unused entirely, or the white cell is forced to gin up data on the spot, which again could throw the game into a failure mode.

Ultimately, for now, the best solution is to be honest about existing limitations and transparent about how any cyber effects are adjudicated. Specifically, in several games, the authors observed an increasing sophistication in cyber tools menus (listed options for attack and defense), and cyber spell cards (weapons held by players to leverage during the game). Again, the idea is not to represent the tools and environment perfectly, but to arrive at an abstraction that allows the game to proceed. Substantial time and treasure are being spent on this problem, and the authors remain cautiously optimistic that better solutions will emerge in the coming years.

Participants, specifically the players and adjudicators, ultimately bear the brunt of the uncertainties and instability in cyber wargaming. Wargames often rely upon player expertise. The problem is that cyber knowledge is not a unified knowledge, nor is it a unified language. This means that cyber experts and practitioners come from across a federated and highly jargonized field. No wargame can afford the endless piecemeal elaboration of institutions all the way down to the tactical edge. Yet, cyber experts with a bigger-picture understanding of the art of the possible are few and far between. In many cases, cyber experts and operators are all the way down in the weeds of the day-to-day threat environment. The result is not just a weedy cyber-practitioner issue. The jargonized and federated understanding of attack and defense can spiral into a complex multi-party collision: government vs. private sector vs. veteran game players. The vocabulary barrier is real, and a serious challenge.

Some cyber expertise is highly segmented and constantly changing. Not even leadership from the major agencies may know who and which agency initiatives are on the rise, and which others have withered on the vine. In part, this is to be expected in gameplay as experts

9 Ibid., 18.

10 Ibid., 21.

learn about the game's elements. But, there are limits to the acceptable instability of the institutional parts. At some point, as the "Wargame Pathologies" report notes, incomplete knowledge on the part of players and the embedded institutional model can fundamentally skew how the interaction unfolds in gameplay. The failure mode for getting the institutional alignments wrong will not only confuse and exacerbate the professionals who agreed to play, but stress the adjudicators and potentially confound the game report.

Ultimately, part of the value of having these wargames is to socialize and learn about all the animals in the cyber zoo—although problematically, this is often not the stated objective. In this sense, those who tout the experiential value of wargaming will point to exactly these kinds of puzzles to explain why cyber wargaming must continue despite the instabilities and the federated knowledge. However, if the actors are constantly shifting along with the domain, the pressure will be on the adjudicators, who are themselves likely only experienced in one of the different knowledge silos.

Solutions? Like everything else here, the authors anticipate that some of the participant issues will resolve themselves over time. Roles and responsibilities across the public and private sector will eventually resolve themselves into a more consistent arrangement of core cyber players and the supporting cyber-adjacent cast. But, game designers can do more than wait. What the authors have witnessed is that designers are easing the load on players and adjudicators by designing better cyber widgets—clever approximations of cyber tools that are simplified enough for players to grasp quickly, but convincing enough to avoid teeing up endless elaboration into the specifics of access, persistence, and exploit.

Given the turbulence of the environment, cyber players will have trouble enough sorting out responsibilities and roles. Leaving out high-fidelity details helps unconfident players feel that they can play cyber, and confident players feel grounded enough not to fight the scenario.

In summary, what the authors have provided here are their early insights as to the state of cyber wargaming through the frame of "Wargame Pathologies." They offer this piece as a starting place for conversation with the practitioner and policy communities. One would do well to recall that, ultimately, the purpose of "Wargame Pathologies" was not to solve problems, but to prepare designers for issues likely to arise. As the inimitable Peter Perla wrote in his canonical book, wargame design is as much art as it is science.[11] This remains true in cyber wargaming, where the dynamics and decisions are frequently assumed to be about computer science and engineering when, in fact, they seldom are. It is, instead, a collective exploration into human decision-making in the context of conflict and cooperation in a domain that, at least by current designs, remains turbulent.

Dr. Nina Kollars is a nonresident fellow with the Atlantic Council's Cyber Statecraft Initiative, and an associate professor of the Strategic and Operational Research Department and a core faculty member in the Cyber & Innovation Policy Institute (CIPI) at the Naval War College.

Professor Benjamin Schechter is an instructor in the Strategic and Operational Research Department and a founding faculty member of the Cyber and Innovation Policy Institute.

11 Peter Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists (Annapolis, MD: Naval Institute Press, 1990).*

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
*Rafic A. Bizri
*Linden P. Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Katie Harbath
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Wendy Sherman
Kris Singh
Walter Slocombe
Christopher Smith
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

List as of January 27, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org