Cyber Wargaming: Grappling with Uncertainty in a Complex Domain

Miguel Alberto Gomez

Senior Researcher

Center for Security Studies

ETH Zurich

Christopher Whyte

Assistant Professor

L. Douglas Wilder School of Government and Public Affairs

Virginia Commonwealth University

Abstract

Cybersecurity literature depends heavily on observational studies to discern state-behavior during periods of conflict. Frequently, underlying motivations that govern the exercise of cyber power are inductively perceived through the lens of the existing strategic environment. While this approach continues to contribute to the advancement of this burgeoning area of study, it is fundamentally constrained by the secretive nature of interstate cyber operations. Moreover, observational studies that analyze state-level actions offer limited insight regarding the individual and group-level mechanisms from which these emerge. The need to move towards these levels of analysis is made even more salient by the uncertainty that permeates this domain that provokes a host of cognitive biases that influence strategic preferences. Consequently, this article offers readers an overview as to the benefits of wargaming as a tool to improve our understanding of crisis decision-making within the cyber domain.

Keywords: *Cybersecurity, Wargame, Experiment, Decision Making*

網路兵推：複雜領域中的不確定性

Miguel Alberto Gomez

資深研究員

蘇黎世聯邦理工學院安全研究中心

Christopher Whyte

助理教授

維吉尼亞聯邦大學 L. Douglas Wilder School 政府與公共事務學院

摘　要

網路安全文獻在很大程度上依賴於觀察研究來識別衝突期間的國家行為。通常，通過現有戰略環境的視角來歸納地認知控制網路力量行使的潛在動機。雖然這種方法繼續為這一新興研究領域的發展做出貢獻，但從根本上，其受到國際網路運營秘密性的限制。此外，分析國家級行動的觀察性研究，對產生這些機制的個人和團體級機制的瞭解有限。滲透到這個領域的不確定性，使這些不同分析層次的需求更加突出，該不確定性引發了許多影響戰略偏好的認知偏見。因此，本文為讀者提供了關於兵棋推演作為一種工具的概述，該工具可以增進我們對網路領域危機決策的理解。

關鍵詞：網路安全、兵棋、實驗、決策

I. Introduction

The past decade has seen the increased usage of cyber capabilities by states to further foreign policy interests. Via the exploitation of the instruments and characteristics of strategic engagement of this human-made domain, belligerent state actors have successfully stolen large volumes of intellectual property, interfered with the operation of critical infrastructure facilities, and influenced the internal political processes of more than two dozen countries. With organizational and technological capabilities advancing year-on-year and with no apparent pause in the exercise of power, the recent characterization of interactions within this space as necessarily persistent appears apt.[1] However, despite most incidents occurring well-below the threshold of armed conflict, the absence of escalation is far from guaranteed.[2] Recent events such as the kinetic response by Israel to Hamas cyber operations, while not a perfect example, highlights the potential for a militarized retaliatory strike. Moreover, with most state-to-state interactions in cyberspace framed in the context of existing rivalry dynamics, the threat of escalation remains a reality should the appropriate conditions come to the fore.[3]

Some would argue that continued interactions between states online should eventually lead to the normalization of "acceptable" and even agreed-upon cyber conflict behavior.[4] Even were that the case,

---

1 Brandon Valeriano and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research*, Vol. 51, No. 3, May 2014, pp.347-360.

2 The lack of escalation may be rooted in the limited effects of these operations.

3 Brandon Valeriano and Ryan C. Maness, *Cyber war versus cyber realities : cyber conflict in the international system* (New York: Oxford University Press, 2015); Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.37-48.

4 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9,

misperception among decision-makers and publics continues to exist as a match that could light the tinderbox of prospective escalation. Misperception may emerge from sudden shifts in strategy between rival states, and the ease of access with which certain actors may obtain offensive capabilities[5] may provoke a shift in the status quo that an opposing party may interpret as a move towards aggression. This situation is further complicated by the inherent uncertainty surrounding the domain that weighs heavily on our inherent cognitive limitations and our dependence on motivated reasoning.[6] Moreover, while the available evidence illustrates the limits of cyber operations relative to their conventional counterparts, biased thinking may result in an inappropriate reaction from those affected by these activities.

Although the complete mitigation of bias is unlikely to occur, acknowledging its presence serves to temper the worst of its effects. At the level of the individuals, this requires one to be aware of what triggers the emergence of this phenomenon and how best to minimize its occurrence. From an organizational perspective, this implies an understanding of both organizational structure and culture that can either decreases or enhances biased thinking. While these lessons may be learned from past failures, adopting this reactive approach is unsuitable given the pace of engagement

---

2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward- constructing-norms-cyberspace.

5 Primarily through illicit markets online. Though this approach does constrain the extent of damage possible. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109.

6 Jacquelyn Schneider, 2017; Miguel Alberto Gomez, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208; Miguel Alberto Gomez and Eula Bianca Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats," *Politics and Governance*, Vol. 6, No. 2, June 2018, pp.61-72.

in cyberspace. Consequently, simulations in the form of wargames provide policy elites and critical organizations the opportunity to observe the effects of biased reasoning and to develop the necessary measures to contain its effects in a controlled environment.

To this end, this article offers readers an overview as to the benefits of cyber wargaming as a tool to improve crisis decision-making. The article progresses by first establishing uncertainty as a crucial characteristic within cyberspace that, in turn, prompts the use of biased reasoning. It then progresses to discussing how wargaming serves as an ideal instrument through which to demonstrate our dependence on these biases and its effects on decision-making. From this point, the article presents readers with the beneficial outcomes of three cyber wargames; the first being a series of annual wargames conducted at the Naval War College, this is followed by a largescale cross-population wargame, and the final simulation being that facilitated by the authors of this article. The article then moves on to provide general guidelines on how readers may develop their cyber conflict wargames and concludes with providing a discussion on the future of wargames in the context of interstate cyber dispute

II. Uncertainty in Cyberspace

A. Technological Uncertainty

Uncertainty is a fundamental characteristic of interstate interactions. Whether it be a question of intent, capabilities, or meaning, the presence of uncertainty constraints our ability to meet the stringent requirements of rational choice.[7] For cyberspace, uncertainty is a function of both the

[7] James D. Fearon, "Rationalist Explanations for War," *International Organization*, Vol. 49, No. 3, Summer 1995, pp.379-414; Dominic Johnson and Dominic Tierney, "The Rubicon theory of war: how the path to conflict reaches the point of no return," *International Security*, Vol. 36 No.1, Summer 2011, pp.7-40; Daniel Kahneman, "A

unique characteristics of this space as well as the strategic environment through which cyberspace is fast becoming an adjunctive instrument of statecraft.[8] Consequently, uncertainty at both these levels facilitates the emergence of biased reasoning from those that respond to cyber incidents.

It is fair to say that cyberspace is the only genuinely human-made operational space. While land, sea, air, and space are, to an extent, malleable, only in cyberspace do we have almost complete control of the laws that govern action and consequences. Although consensus regarding the exact nature of cyberspace continues to elude us, we can characterize this space as consisting of three unique yet interdependent levels: physical, syntactic, and semantic.[9]

The physical level is best described as consisting of the hardware that allows for the transmission and processing of data as either electrical signals, pulses of light, or waves within the electromagnetic spectrum. This level encompasses the physical hardware that allows computation to take place. Above this is the syntactic level that is governed by unique protocols that enable computers to process the transmitted signals. Artifacts such as operating systems and applications exist at this layer. These protocols allow for interoperability across different manufacturers. Finally, the semantic represents the human-readable information itself that can be presented within a standalone environment (e.g., a PDF document on your computer)

---

perspective on judgment and choice - Mapping bounded rationality," *American Psychologist*, Vol. 58, No. 9, September 2003, pp.697-720.

8 Benjamin Dean and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy," *Penn State Journal of Law & International Affairs*, Vol. 5, No. 1, April 2017, pp.29-71; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017); Brandon Valeriano, Benjamin Jensen and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

9 Martin C. Libicki, *Cyberdeterrence and cyberwar* (Santa Monica, CA.: Rand Corporation, 2009).

or in a networked space (e.g., posts on Facebook).

To demonstrate the functionality of these levels, imagine how an e-mail is sent. A sender first decides on a specific message to transmit and then types this into an e-mail client (Semantic). The e-mail client then formats this message per the transmission protocol (Syntactic). Once formatted, the computer then transforms this information into electromagnetic signals to be sent across a network such as the Internet to the recipient (Physical). Once received, the recipient's computer then reconstructs these signals into the appropriate format as required by the protocol (Syntactic), which the e-mail client then presents to its user in a human-readable form (Semantic).

Despite the seeming simplicity of the above process, uncertainty emerges through several mechanisms. Foremost among these is the overall complexity of cyberspace given the linkages between individual computers and networks operating within this space. This interconnectedness increases overall complexity that limits our ability to predict points of failure and its corresponding consequences.[10] Moreover, this sense of unknowability is further aggravated by the concern – merited or otherwise – of the possibility of cascading effects between the three levels.[11] For instance, a disruption in the Physical level will undoubtedly affect our ability to transmit signals between two points that eventually affect both the Syntactic and Semantic levels as well. Similarly, the manipulation of the protocols governing the Syntactic level can result in incorrect information being presented at the Semantic level.

---

[10] Charles Perrow, *Normal accidents: living with high-risk technologies Princeton paperbacks* (Princeton, NJ.: Princeton University Press, 1984).

[11] Ilai Saltzman, "Cyber posturing and the offense-defense balance," *Contemporary Security Policy*, Vol. 34, No. 1, March 2013, pp.40-63; Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

Further complicating this situation is the persistent lack of expertise concerning this domain. Hansen and Nissenbaum[12] argue further that this lack of domain expertise contributes to the hyper-securitization of cyberspace, further contributing to notions of "cyber doom" as a result of malicious behavior aimed at critical infrastructure. This exaggeration of effects is apparent in a study by Jarvis, Macdonald, and Whiting[13] that demonstrate the persistence of headlines over the past decade that frame cybersecurity incidents through these apocalyptic analogies.

While the use of analogies is a common cognitive short-cut that allows aids in the comprehension of a complex phenomenon in uncertain situations, bias ensues when it fails to depict reality accurately. The use of analogies during periods of political crisis is relatively common, references to Munich or Pearl Harbor tend to surface in response to autocratic leaders or periods of surprise. However, the context between the original events and their intended parallels are rarely mirror images of one another. As a result, the lessons from those cases may not be wholly suitable for the present.[14]

In the context of cyberspace, events akin to 9/11 or Pearl Harbor have yet, if ever, to occur.[15] The exercise of cyber power resulting in first-order

---

[12] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4, December 2009, pp.1155-1175.

[13] Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat," *European Journal of International Security*, Vol. 2, No. 1, February 2017, pp.64-87.

[14] Robert Axelrod, "A Repertory of Cyber Analogies," in Emily O. Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Dept. of Defense Information Operations Center for Research, 2014); Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ.: Princeton University Press, 1992).

[15] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

effects that result in the loss of life.[16] Furthermore, the idea of a sustained assault on an adversary's cyber infrastructure that would force a regime and its populace to yield is unlikely given the immense resource requirements and the availability of conventional alternatives.[17] However, despite the available evidence, political elites continue to promote the idea of an apocalyptical attack against critical cyber infrastructure that, in turn, result in increasingly aggressive strategies being developed.[18]

B. Strategic Uncertainty

Apart from technical considerations, uncertainty is also associated with the strategic environment in which cyber power is exercise. Although early advocates promoted the idea of the domain's a-strategic nature, empirical evidence highlights the strategic context in which interstate interactions within this space takes place.[19] Maness and Valerianio note that cybersecurity incidents often occur between established rivals within a given region.[20] Rarely do we observe cybersecurity incidents occurring without a preexisting strategic cause, whether this be political, economic, or military. Furthermore, both authors argue that exchanges between these rivals are also characterized by stability resulting from past interactions with one another. While this suggests a degree of understanding between adversaries, uncertainty can still emerge through capability acquisition,

---

[16] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp.5-32.
[17] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3, May 2017, pp.452-481.
[18] The 2018 United States strategy best represents this shift towards increased aggression and engagement. USA. "National Cyber Security Strategy of the United States of America," 2018.
[19] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013).
[20] Op. cit, pp.347-360.

perceived intent, and motivated reasoning.[21]

An enduring myth surrounding the exercise of cyber power is the notion of the low cost of entry into this space.[22] While it is easy to trace the roots of this belief to the ready availability of capabilities, it should be noted that the utility gained from its usage is directly proportional to the resources spent on its development.[23] Phrased another way, while tools to take down websites or botnets to conduct Distributed Denial-of-Service attacks are easily accessed, the ability to inflict lasting damage requires additional investment.

On the surface, this suggests that truly damaging attacks are limited to a handful of actors with the appropriate material and organizational resources to mount an effective attack. However, a shift from the status quo due to the appearance of new capabilities may trigger a security dilemma between rivals despite the actual effects.[24] This is particularly true if the targets are increasingly dependent on cyberspace. Cognitive phenomenon such as the endowment effect and negativity bias can prompt an overreaction on the part of the targets regardless of the actual damage suffered.[25] This situation could encourage the slighted party to develop capabilities to operate in cyberspace – further destabilizing the precarious balance.

---

[21] Buchanan, Op. cit.

[22] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109; Op. cit., pp.452-481; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3, July 2013, pp.365-404.

[23] Adam Liff, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war," *Journal of Strategic Studie*s, Vol. 35, No. 3, June 2012, pp.401-428. Ibid.

[24] Buchanan, Op. cit.

[25] Dominic Johnson and Dominic Tierney, "Bad World: The Negativity Bias in International Politics," *International Security*, Vol. 43, No. 3, February 2019, pp.96-140.

Apart from the acquisition of capabilities, the exercise of such also raises questions of intent. The use of conventional weapons is commonly associated with destructive intent. Malicious code, however, serves to establish a foothold in a privileged system to either exfiltrate privileged information or cause damage at a later date. This characteristic of dual-usage opens up the possibility for misperception on the part of the target that is further aggravated by the system affected.[26] A compromise of the national tax system may be of limited consequence while gaining access to a state's Nuclear Command, Control, and Communications (NC3) would have genuine consequences.

This ambiguity of intent is further worsened by the emergence of motivated reasoning that individuals may use to explain events in the absence of complete information while still maintain pre-existing beliefs.[27] Since interactions in cyberspace are strategic in nature, past experience may serve to frame actions in the present. If an adversary demonstrated belligerence in the past, an enemy image[28] might exist to inform judgments in the present.[29] Moreover, since individuals tend to maintain beliefs rather than expend precious cognitive resources to re-evaluate them, it seems likely that a target may perceive this incident as an attempt by an adversary to further its interests at the cost of the target. In conjunction with limited

---

[26] Op. cit., pp.37-48; Buchanan, Op. cit.

[27] Ziva Kunda, "The case for motivated reasoning," *Psychological Bulletin*, Vol. 108, No. 3, December 1990, pp.480-498; Robert Jervis, *Perception and misperception in international politics*. New edition. ed. (Princeton, NJ.: Princeton University Press, 1976); Robert Jervis, "Understanding beliefs and threat inflation," in Trevor A. Thrall and Jane K. Creamer, eds., *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11,* (Abingdon-on-Thames, UK: Routledge, 2009), pp. 16-39.

[28] Preconceived notion of how a potential adversary behaves based on past cases.

[29] Ole R. Holsti, "The Belief System and National Images: A Case Study," *The Journal of Conflict Resolution*, Vol. 6, No. 3, September 1962, pp.244-252; Ole R. Holsti, "Cognitive Dynamics and Images of the Enemy," *Journal of International Affairs*, Vol. 21, No. 1, 1967, pp.16-39.

familiarity with cyberspace and the use of analogies, the destabilization of the status quo is perceived to be more likely as a result of this biased reasoning.

C. Real-World Cases

While it would be easy to dismiss the logic previously laid out, several real-world cases demonstrate biased reasoning stemming from some of the mechanisms established previously. Incidents such as Solar Sunrise, the Estonia DDoS, and the Pyeongchang Olympics highlight the emergence of biased reasoning.

Over three weeks in February 1998, the United States Department of Defense suffered a series of attacks against its unclassified computer networks. These incidents utilized several known operating system vulnerabilities that allowed for the exfiltration of data. The sources of the attacks appeared wide-spread and were thought to have originated from countries such as Israel, the United Arab Emirates, France, etc. These attacks occurred when the United States was preparing possible military action against Iraq due to weapons inspection issues. As such, it was initially assumed that the source of these incidents was the Iraqi regime, given the timing and surrounding strategic context. Later analysis revealed, however, that teenagers in the United States and Israel were responsible.[30]

Similarly, the massive Distributed Denial-of-Service attack against Estonia in 2007 appears to highlight biased reasoning on the part of political elites when attributing the incident to the Russian Federation. Stemming from the decision to move a World War II Memorial, Estonia experienced a series of attacks that disrupted government and financial systems. Based on

---

[30] Richard Power, "The Solar Sunrise Case: Mak, Stimpy, and Analyzer Give the DoD a Run for Its Money," *informit*, October 30, 2000, http://www.informit.com/articles/article.aspx?p=19603&seqNum=4.

reports leaked through the whistleblower website WikiLeaks, it appears that Estonian officials cited both the benefits gained by Russia and their previous actions as justifications for this incident. Furthermore, despite later forensic analysis, the Estonia leadership appeared reluctant to change their belief even with the presence of disconformity evidence.[31]

Finally, the opening ceremonies for the 2018 Pyeongchang Olympics were disrupted by a cyber attack. Early assessments appeared to have attributed the incident to North Korea, given the underlying strategic context. This, however, was later found to have been a false flag operation.[32]

While authors such as Harknett and Fischerkeller argue that persistent engagement would result in a better understanding between adversaries,[33] this possible socialization alone cannot address our concern with biased reasoning. Knowing how adversaries behave does not remove the inherent uncertainty associated with the nature of the domain. Moreover, further socialization cannot wholly address shifts in behavior or the questions of intent with the appearance of malicious code. Consequently, learning from the past is a necessary but not sufficient means of addressing biased

---

[31] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, Last Modified May 17, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html; USGOV. 2007a. "Estonia's Bronze Soldier: It's Deja Vu All Over Again," WikiLeaks, Last Modified 16.02.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN106_a.html; USGOV. 2007b. "Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State," WikiLeaks, Last Modified 04.06.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN366_a.html.

[32] Paul Rascagneres and Martin Lee, "Who Wasn't Responsible for Olympic Destroyer?" Talos Intelligence, February 26, 2018, https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html.

[33] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

reasoning in this increasingly conflict-prone space.

III. Surfacing Bias Through Wargaming

Simulations such as wargames are frequently utilized as a pedagogic or evaluative instrument. The former as a means of demonstrating a particular concept while the latter serves to assess the efficacy of a given plan. However, this instrument can also be called up as a means to investigate, demonstrate, and address the shortcomings of dynamic decision-processes that emerge in high-stress environments.

A. Suspension of Disbelief

Despite its fictitious origins, wargames provide participants with an environment in which equivalent real-world decision-making processes are surfaced for evaluation. A key enabler being the narrative format that wargames typically adopt. As noted by Perla and McGrady,[34] the suspension of disbelief that is fundamental to the success of these simulations depend on the differences between the "automatic" and "systematic" cognitive processes at work. The former is typically associated with adaptive processes that serve to provide an immediate assessment of a given situation with minimal cognitive resources. At the same time, the latter is typified by more deliberative reasoning that, in turn, requires considerable cognitive effort.[35] Procedurally, the former precedes the latter when we process information.

Consequently, the suspension of disbelief required to allow participants to behave as they would in the real-world hinges on the ability to suppress these systematic processes. Neurological research suggests that the

---

[34] Peter P. Perla and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No.3, Summer 2011, pp.111-130.

[35] Daniel Kahneman, *Thinking, fast and slow.* 1st ed. (New York: Farrar, Straus and Giroux, 2011).

activation of these systematic processes is tied to the extent to which real-action is required in response to the information provided. That is to say, when presented with a narrative such as that contained in a wargame scenario; its success rests on our ability to respond in the real-world. Without such, automatic processes enable us to engage in the narrative without questioning its authenticity.[36]

As an example of these processes, students were presented with two accounts concerning the career of the first president of the United States, George Washington. The first contains a factual account of how Washington become the first president. The second employs dramaturgical techniques to introduce a degree of uncertainty as to whether or not he would be elected into office. Those exposed to the latter took longer to answer whether or not he was indeed elected as the first president. The author believes that even though these participants were well aware of who the first president was, the ambiguity in the construction of the narrative made the students believe otherwise (albeit briefly) before the engagement of "systematic" processes.[37]

This phenomenon enables designers to frame an environment in which participants are convinced to behave in a manner that parallels the real-world. This, in turn, allows us to observe decision-making processes that would otherwise be inaccessible due to administrative requirements (i.e., security clearance requirements) or probabilistic constraints (i.e., rare events).

---

[36] Norman N. Holland, "Spider-Man? Sure! The neuroscience of suspending disbelief," *Interdisciplinary Science Reviews*, Vol. 33, No. 4, December 2008, pp.312-320.
[37] Richard Gerrig, *Experiencing Narrative Worlds* (New York: Routledge, 2018).（Ebook）

B. Minimizing Risks, Encouraging Actions

The ability to shape reality and the extent to which these are believed to be fact enables participants to act accordingly without fear of consequences. This is not to say that consequences are omitted outright; instead, designers can shape these consequences in a manner that best suits their needs. For instance, in studying whether or not cybersecurity incidents prompt decision-makers to gravitate towards information that would provide immediate closure as a function of their role; designers may limit consequences on a participant's continued position of a given role (e.g., being voted out of office due to his or her failure to act).[38] In effect, this is akin to the application of specific treatments within an experimental design.

Assuming that the narrative is effective in suspending disbelief, designers can introduce features such as specific consequences or the availability of information that would elicit the processes described in the previous section. In turn, this could trigger biased judgments that would typically occur in the real-world without the corresponding real-world effects discouraging.

This is the crux of this article's argument. The ability to convince wargame participants that the environment they are operating in is similar to that in the real-world allows parallel actions and decisions to be enacted. This being a constructed space, designers introduce features that trigger specific cognitive or affective responses that result in the emergence of bias. These and their effects are observed throughout the gameplay and are then communicated to the participants as part of the debriefing activity. It is at this point that participants, with perhaps the assistance of the game designers, can design processes that would mitigate the worst effects of

[38] Arie W. Kruglanski and Donna M. Webster, "Motivated closing of the mind: "Seizing" and "freezing"," *Psychological Review*, Vol.103, No.2, April 1996, pp.263.

based judgments under real-world conditions.

C. Pitfalls of Wargaming

While the previous subsections appear to frame wargames as a panacea for addressing biased decision-making, these are not without their limitations. Designers could fail by either under/overestimating certain conditions in the fictitious narratives or may provide an over-simplified scenario due to complexity issues or a lack of knowledge.

It is not unheard of for designers to misrepresent the likelihood of threats and the severity of consequences. High-profile simulations have fallen into this trap resulting in the emergence of inappropriate policies.[39] For cybersecurity, the potential for this is very much a reality given the opaque nature of events. Events such as the annual Cyber 9/12 Challenge depict conditions that, while engaging for participants, may not necessarily be representative of real-world conditions.[40] While such a representation may still result in the emergence of specific biases, these would not necessarily be identical to those observed under real-world conditions.

Relatedly, designers can also fall into the trap of oversimplifying the narratives presented in the course of wargames. Oversimplification, however, may not always be unintentional. If the objective is to understand the specifics of a given process, the omission of certain aspects could provide additional analytic clarity that better serves the intent of the designers. Unfortunately, oversimplification may also emerge from a lack of understanding concerning real-world processes and may or may not be addressable. In any event, simplification may prevent specific processes

---

[39] Tara O'toole, Mair Michael, and Thomas V. Inglesby, "Shining light on "Dark Winter"," *Clinical Infectious Diseases*, Vol. 34, No. 7, April 2002, pp.972-983.

[40] This is not a failure on the part of the designers but to provide an engaging and thought-provoking scenario on the part of the participants who are mostly students.

from being observed when these omitted variables are crucial for their emergence. For instance, assuming the absence of small-decision groups and assigning individuals as the sole decision-maker would not allow group dynamics to unfold that contribute to the effects of specific biases.

Ultimately, designers should be cognizant of the limitations inherent in their scenarios. The opaque nature of cybersecurity is unlikely to yield a perfect representation of the threat, and the complex nature of this environment can make a faithful reproduction within a simulated space prohibitively expensive. Nevertheless, by keeping these in mind, designers can account for the extent to which these wargames simulate reality, and the overall utility offered to participants.

IV. Notable Cyber Wargames & Key Observations

The appearance of wargaming as a crucial instrument has come to the fore given limited access to elite decision-making artifacts during periods of conflict. More importantly, the growing popularity of wargaming allows researchers to evaluate better the extent to which uncertainty and biased reasoning interact, resulting in sub-optimal judgments on the part of military and political elites. In recent years, interest has formed around the study of the psychological aspects of cybersecurity.[41] Although experimental designs demonstrate the importance of this micro-level approach and the potential for sub-optimal judgments, these observations are drawn from non-elite samples that may differ from individuals exposed to real-world

[41] Miguel Alberto Gomez, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208; Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.49-58; Miguel Alberto Gomez, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

incidents.[42] The rise of wargaming, as such, offers a means through which these experimentally derived observations are either validated or refuted. While larger events such as the annual Locked Shields (CCDCOE 2019) exercise by NATO are typical of these activities,[43] little has been said regarding specific patterns of behavior exhibited by participants.[44] Taking into consideration the objectives of this article, it briefly recounts the research conducted by Schneider, Jensen and Valeriano, and Gomez and Whyte.[45] The three are comparable in the sense that these articles focus on elite decision-making vis-à-vis the escalatory risks associated with cyber operations.

Serving as an entrepreneur with respect to cybersecurity wargaming, Schneider discusses the data obtained from the wargames conducted at the United States Naval War College from 2011 to 2016.[46] These activities took the form of table-top exercises wherein elite participants[47] were presented scenarios involving disputes with near-peer or asymmetric adversaries that occurs within one of the conventional domains (i.e., land or sea). These individuals (blue team) interacted with the adversary (red team) that is role-played by another set of elites. Consequently, these wargames take the form of an open-play type exercise.[48]

Before proceeding further, it is essential to note the critical difference

---

[42] Alex Mintz, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

[43] CCDCOE, "Locked Shields 2019," CCDCOE, https://ccdcoe.org/exercises/locked-shields.

[44] Although reports have emerged from these events, scientific analysis is limited, if at all present.

[45] Jacquelyn Schneider, 2017; Benjamin Jensen and Brandon Valeriano, "The Cyber Character of Crisis Escala," presented at the International Studies Association Annual Convention (Toronto, March 27, 2019); Miguel Alberto Gomez and Christopher Whyte, 2019.

[46] Ibid.

[47] Military and government officials.

[48] No pre-structured/pre-planned response based on the participants' actions.

between her study and the other two as it frames the generalizability of the findings. First, the wargames Schneider analyzes is not an exclusively cyber-on-cyber exercise. Instead, cyber operations are treated as one of the policy options available to participants. This is crucial as the findings cannot be said to apply directly to situations where interactions remain exclusively within cyberspace. On the other hand, it does realistically depict the cross-domain nature of interstate interactions in the modern interstate system.[49] Second, these wargames were not designed as experiments such that specific behavioral outcomes cannot be ruled out as the effects of confounding variables. This limitation, however, is offset by the fact that the scenarios and participants remain relatively consistent across this period and limit the impact of confounders.

That being said, Schneider makes several noteworthy observations regarding behavior during periods of crisis. Foremost among these is the belief in the escalatory nature of cyber operations that limited both cyber exploitation and information operations. When these were considered, the emphasis was placed on the need to ensure reversibility and non-attribution. Moreover, it was observed that analogies were drawn between cyber operations and nuclear capabilities but none between these and conventional weapons. These observations, at least at the time of the wargames, are significant for conceptual and pragmatic reasons. Conceptually, the conflation between cyber and nuclear speaks to the continued prevalence of the "Cyber Doom" scenario in which cyber operations are believed to have significant escalatory potential such that the mere discovery of these (even if solely for espionage) could signal an intent to escalate.[50] Pragmatically,

---

[49] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2, April 2016, pp.301-323.

[50] Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.37-48; Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017).

these findings demonstrate alignment with existing strategic considerations at the time. Before the 2018 version of the Department of Defense Cyber Strategy, restraint was reflected in past strategic documents.[51] Although the wargame cannot definitively confirm it, this perceived escalatory potential of cyber operations may have influenced the framing of strategic thought and documents at the time.

Inversely, the wargames also highlighted a cross-over point in which cyber operations were perceived to be less escalatory. Except for a single case, cyber operations are thought to be less escalatory only once conventional operations were initiated. This observation is relevant given that most real-world cyber operations aimed at the United States, and others occur well before armed conflict is initiated. These results highlight the importance of emotions in the formulation of judgments that later inform policy decisions. Schneider notes that anxiety, rather than fear, may account for the absence of escalatory tendencies on the part of the participants.[52] Unlike fear that provokes a hardening of one's position, anxiety may manifest as risk-averse behavior, much like that observed in the series of wargames noted in the study.[53] Furthermore, while the article is unable to surface the role of emotions definitively, these findings find support in published research on the importance of emotions in response to incidents in cyberspace.[54]

---

[51] Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

[52] Schneider, op. cit.

[53] Paul J. Whalen, "Fear, Vigilance, and Ambiguity: Initial Neuroimaging Studies of the Human Amygdala," *Current Directions in Psychological Science,* Vol. 7, No. 6, December 1998, pp.177-188.

[54] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No.1, March 2017, pp.49-58.

Following up on their findings, Jensen and Valeriano (2016) are conducting a series of wargames in the context of an experimental study. Whereas cyber operations were not the primary policy response of interest in the wargames evaluated by Schneider, Jensen, and Valeriano are instead interested in how the expression of power within this human-made domain either encourages or mitigates escalatory risks among parties involved.

For these authors, the wargames involve peer rivals currently embroiled in a territorial dispute with each other. The authors then manipulate the underlying conditions along two dimensions. First, a recent issue necessitating a response (does or does not) involve an offensive cyber operation by one of the parties. Second, those reacting to this incident (do or do not) have a cyber operation as one of several possible response options. This design allows the authors to isolate the effects of both factors on decision-making and the propensity for bias. To maximize the generalizability of their findings, the authors recruited participants from the government, academia, and industry.

Although the study is yet to be completed, the initial findings are proving to be significant. Cyber operations do not appear to increase the risk of escalation in a militarized dispute. Matching Schneider's earlier findings, the exercise of cyber power once conventional means have been employed does not appear to be provocative. In line with this, participants with the option to respond via cyber means are less escalatory than those without. Phrased differently, lacking the ability to respond in kind, targets of cyber operations opt to escalate into the physical domain in order to demonstrate resolve.

The policy implications of these findings are crucial. If cyber operations do not affect the strategic calculus between rivals engaged in a militarized dispute, then escalation should not be of significant concern. A similar pattern was observed in a recent article by Kostyuk and Zhukov that explored the escalation associated with cross-domain engagements in the

ongoing dispute between Ukraine and Russia.[55] On the other hand, it is essential to note that operations to date have limited physical effects. Should this change, the escalatory calculus may respond in kind.

Furthermore, this finding does not speak much about the dangers of collateral damage beyond the intended target, possibly inviting a response from an unintended target. Schematic reasoning that may emerge due to the continued use of cyber operations owing to its "limited effects" may lead to a less deliberate justification of its use in the future. The recent introduction of the United States' persistent engagement model harkens to this issue. Although the United States may view sustained cyber operations as a necessity with limited escalatory risk, its justification for this strategy may simply be a product of mirror imaging bias rather than deliberative reasoning.

While the design offered by Jensen and Valeriano is a step in the right direction, it does suffer from the limitation that intra-group dynamics do not appear to have been taken into consideration. Although the scenario is tackled as a group, the authors do not provide insight into the dynamics resulting in the final decision. This is an essential limitation as groups can either mitigate or enhance individual-level biases.

Finally, research conducted by Gomez and Whyte tackles the question of escalation from the point of view, distance, and temporality.[56] As with Jensen and Valeriano, their research tackles the issue through an experimental design. An initial large-N survey experiment is conducted on

---

[55] Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *The Journal of Conflict Resolution*, Vol. 63, No.2, February 2019, pp.317-347.

[56] Miguel Alberto Gomez and Christopher Whyte, 2019; Distance refers to the proximity of an actor to the effects of an operation while temporality is the urgency associated with responding to the said event.

(non-elite) individuals from Five Eyes member states.[57] Because of the nature of the participants, a follow-on wargame matching the initial survey experiment was conducted with the Institute for National Defense and Security Research (INDSR) in Taiwan to strengthen the generalizability of the findings. It should also be mentioned that unlike the experimental design adopted by Jensen and Valeriano, this wargame attempts to establish the effect of organizational structures have on decision-making. Instead of having a group decide as a single individual, participants assume specific roles and are given privileged information as determined by their role.[58] While not explicitly instructed to do so, participants are free to withhold information from the rest of the group – thus increasing uncertainty commonly observed in these incidents.

A key differentiator between this and that of the former two is the exclusivity of cyberspace in the scenario. Wherein Schneider and Jensen and Valeriano framed their first scenario as disputes occurring within the conventional domains, the issue prompting the use of cyber operations is that of cyber operations targeting the media and critical infrastructure. This design choice has both inherent weaknesses and strengths. On the one hand, this reduces the wargame's overall realism. As issues beyond the domain often initiate most interstate interactions in cyberspace, it is possible that more informed participants are unable to suspend their disbelief and thus fail to commit fully to the scenario. On the other hand, this allows the authors to isolate the decision-making processes that may give rise to bias in cases where disputes are grounded solely on malicious behavior in cyberspace.

A key finding of this wargame is the dependence on pre-existing

[57] Participants are limited to those of the Five Eyes to control for variation owing to culture of threat perception vis-à-vis cyberspace.
[58] Policy Expert, Military Expert, and Cybersecurity Expert.

beliefs in formulating decisions in response to cyber operations. Theoretically, these findings align with current social and cognitive psychology literature. When faced with uncertainty, individuals fall back on readily available concepts and frame their judgments within the bounds of these structures.[59] While these cognitive mechanisms allow for an efficient assessment of the situation, overreliance is likely to result in biased judgments. In one case, a team decided to yield to the demands of an adversary due to the value/importance they have on preserving human life. However, as valid and noteworthy as this may be, the influence exerted by this belief limited their ability to realize the negative signal this may send to potential adversaries in the form of perceived weakness. Apart from this, the results also highlight the importance of information, as seen in the intra-group dynamics and the justification of their actions. Less knowledgeable individuals actively sought out information from more knowledgeable members of their team. Barring that, assumptions were made based on their understanding of past incidents and their expertise.

The importance of pre-existing belief and domain expertise expressed by the participants reflects earlier findings by both authors. Whyte (2016) notes that the failure of the coercive operation by North Korea against the United States is linked to the former's underlying beliefs (i.e., liberal-democratic values) and its influence on the decision to resist North Korean demands.[60] Similarly, both belief systems and domain expertise weigh heavily in a series of experiments that investigate the attribution of cyber operations. Enemy images, in particular, provoke schematic thinking through which decision-makers preempt available evidence and form narratives (whether or not these conform to reality) that serve to explain an

---

[59] Deborah Welch Larson, "The Role of Belief Systems and Schemas in Foreign Policy Decision-Making," *Political Psychology*, Vol. 15, No.1, March 1994, pp.17-33.

[60] Christopher Whyte, "Ending cyber coercion: Computer network attack, exploitation and the case of North Korea," *Comparative Strategy*, Vol. 35, No. 2, March 2016, pp.93-102.

adversary's current and future actions.[61]

The above findings reflect significant policy implications. An overreliance on beliefs constraints the search for information and potentially discounts the negative consequences of specific actions. The search for information and a reliance on experts may, in turn, may disproportionately increase the influence of an individual or sub-organization in the decision-making process. Consequently, this may result in policies driven primarily by parochial interests rather than the overall well-being of the organization or state.

Although the above wargames vary in terms of design, the observations derived from these contribute significantly to our understanding of decision-making in this domain. More importantly, the intersections of the above findings with those derived from observational and experimental research point to the importance of wargaming in broadening our understanding of actors within cyberspace. These highlight the genuine possibility of bias stemming from the uncertainty associated with events in cyberspace. With the utility offered by cyber wargames established, the remainder of this article provides a general guideline on how best to design these activities of research or training purposes.

V. Designing Cyber Wargames

It is crucial to note that despite its history and frequent use, no clear guidelines exist on how best to design wargames. More so for those tailored for the domain of state-level cybersecurity. While this article does not aspire to establish clear rules as to how best to engage in this endeavor, it proffers vital considerations that should go into the conceptualization, development,

---

[61] Miguel Alberto Gomez, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

and execution of cybersecurity wargames. Readers should be aware that cybersecurity wargames conducted at the strategic rather than operational level, which are the focus of this article, are not fundamentally different from those that involve the conventional domains of air, land, and sea. The introduction of uncertainty to simulate real-world conditions is achieved either explicitly through the manipulation of the underlying organizational and/or strategic relationships amongst the participants and implicitly by the very nature of the simulated cyber environment.[62] Consequently, the extent to which biased and sub-optimal decisions are surfaced depends on the preceding manipulation. The careful manipulation of these attributes allows game designers to better approximate real-world conditions that elicit useful observations.

A. Overall Objective

What purpose does the wargame serve? Mundane as this question may be, it serves as the cornerstone for any planned wargame – cyber or otherwise. Wargames serve to either test the feasibility of existing plans, the readiness, and capabilities of specific groups or to identify specific decision-making behavior and shortcomings. Although wargames would share common features, their specific function dictates the structure, flow, and ultimate utility of these activities.

For instance, those designed to test pre-existing plans contribute significantly to understanding whether or not an organization currently possesses the capabilities to face certain eventualities but is unlikely to demonstrate improvisational capabilities. Similarly, those structured to compare the performance of different groups are unsuitable if the designer

---

[62] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

intends to observe cooperative behavior between these groups.

Consequently, the objectives of these activities must be established before further steps being taken. This does not only increase the value of the activity but may assist in reducing unnecessary administrative overheads and resource expenditures.

B. Level of Play

One crucial point to acknowledge when designing cyber wargames is the level at which the wargame takes place. In the context of cybersecurity, this can occur either at the operational or strategic level. Wargames at an operational level are technical and serve to evaluate the ability of operational teams to react to an individual or related technical incidents independent of the overall strategic context. In contrast, strategic games involve the exclusive or adjunctive use of cyberspace in a broader strategic environment. Games of this type require cybersecurity incidents to be evaluated not only on a technical but on political, economic, and/or military aspects as well. The decision to engage in either of the above types requires special considerations in terms of resources and expected findings.

Operational-level cyber wargames, to be as realistic as possible, require the use of a dedicated network(s) through which participants may engage in offensive and defensive acts. This requires significant material resources and technical expertise to design, deploy, and evaluate. From an analytical perspective, these events are useful in evaluating the extent to which operational elements of an organization is effective in dealing with an individual or related security incidents.[63] However, higher-level decision-makers are usually not involved, and, as such, the observations

[63] These types of events are fairly common in the Information Security field in which individuals and/or groups are evaluated on their skill level or adherence to specific standards such as the NIST Cyber Security Framework.

gained are limited.

Strategic-level cyber wargames, in contrast, can be limited to a table-top exercise or extended to include an operational aspect as well given available resources. Unlike the above, these games also involve vital decision-makers that are responsible for high-level policies (e.g., foreign policy experts). Involving them in the process allows the designers to better replicate real-world incidents in which operational-level individuals provide strategic decision-makers with information necessary to make policy decisions. However, care must be taken in providing a balance between realism and analytical reality.

Although both operational and strategic-level wargames are useful in understanding organizational behavior, the choice between the two depends on the overall objectives of the game designer. Moreover, the decision also influences other considerations discussed in the succeeding subsections.

C. Participant Identification

Once the wargame objective is established, the makeup of its participants should also be considered. Fundamentally, the identity of game participants is a function of both the game objectives and access granted to designers. Keeping these in mind is crucial as it contributes directly to the practicability of the game itself as well as the generalizability of the data gathered throughout gameplay.

Participants in a wargame can either be elite or non-elites. Elites, in this case, refers to individuals with specific real-world roles that correspond directly to some aspect of the game. For instance, a military officer may play the role of the chairman of the Joint Chief of Staff in a game that attempts to simulate the upper levels of the United States Government. In contrast, non-elites are individuals who better represent the general public as a whole. The use of students serves to exemplify this case. As a question of practicality, the decision to favor one group over another in the conduct of a

wargame is a matter of access. Beyond this, however, participant background also has crucial theoretical implications that could have a serious bearing on how these individuals interact with the activity and the informative value offered by their observed actions.[64]

The decision to select elites or non-elites is influenced by the task assigned to them and the level of expertise required. Tasks not requiring specialized knowledge or expertise, such as the formation of judgment and initial perceptions, renders the distinction between experts and non-experts moot. By their nature, these tasks tap into cognitive and psychological processes that are either common to most individuals or are easily induced through experimental manipulation.[65] At worst, the decision to employ non-elites may result in less pronounced effects compared to that of elites.[66] The difference, however, can be accounted for during evaluation by citing real-world equivalents or other related cases. In contrast, structured tasks may require familiarity with real-world processes or situations inaccessible to non-elites. This distinction suggests a clear difference between how the former would behave in a wargame compared to that of the latter.

---

[64] Emilie M. Hafner-Burton, Alex D. Hughes, and David G. Victor, "The Cognitive Revolution and the Political Psychology of Elite Decision Making," *Perspectives on Politics*, Vol. 11, No.2, June 2013, pp.368-386; Alex Mintz, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

[65] Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment under uncertainty: heuristics and biases* (New York: Cambridge University Press, 1982); Paul Slovic, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "The Affect Heuristic," *European Journal of Operational Research*, Vol. 177, No. 3, March 2007, pp.1333-1352.

[66] Richard R. Lau and David P. Redlawsk, "Advantages and Disadvantages of Cognitive Heuristics in Political Decision Making," *American Journal of Political Science*, Vol. 45, No.5, October 2001, pp.951-971; Joshua D. Kertzer and Kathleen M. McGraw, "Folk Realism: Testing the Microfoundations of Realism in Ordinary Citizens," *International Studies Quarterly*, Vol. 56, No.2, June 2012, pp.245-258; Elizabeth N. Saunders, "No Substitute for Experience: Presidents, Advisers, and Information in Group Decision Making," *International Organization,* Vol. 71, No. S1, April 2017, pp.219-247.

D. Group versus Individual Gameplay

Apart from individual participant backgrounds, in-game interactions (or the lack thereof) require consideration relative to the modeled real-world processes. While decision-making can be easily left to the individual, most state-level actions are the result of group dynamics. Even in the most autocratic of regimes, decisions may still be the result of small group dynamics. Although game designers may opt to delegate this process to an individual for either administrative (e.g., time) or design (e.g., complexity) constraints, this risks the failure to capture particular dynamics that only appear within a group setting.

For instance, cognitive biases are either aggravated or mitigated through interpersonal interactions. Groupthink could surface, thus allowing the propagation of biased and sub-optimal thinking. Inversely polythink could emerge, thus resulting in a less biased decision on the part of the group.[67] In either case, limiting game-play to individuals comes at the cost of allowing these processes that frequently occur in the real-world to unfold. This does reduce not only the overall realism of the exercise but also limits its overall generalizability.

This is not to say, however, that all wargames and related simulations should be done as a group. Instead, we argue that gameplay should take into consideration aspects of the environment being replicated. Furthermore, concerning this article's focus on complexity resulting in biased decision-making, developing an environment wherein these mechanisms manifest themselves is crucial if the objective of the designers is to understand decision-making processes better.

E. Level of Engagement

[67] Alez Mintz and Carly Wayne, "The Polythink Syndrome and Elite Group Decision-Making," *Political Psychology*, Vol. 37, No. S1, February 2016, pp.3-21.

Wargames can either be designed to progress based on a pre-determined ruleset or to flow more naturally through free-play (e.g., Red Team versus Blue Team).[68] While one is not necessarily better than the other, selection would depend primarily on the underlying objectives of the game. With the increasing use of games as a pseudo-experimental method, this decision cannot be made lightly.

Although allowing the game to develop through a series of pre-determined rules, possibly leading players towards the win condition is experimentally preferable, this denies players the freedom of action that would be common in a real-world setting. In contrast, free-play increases the overall realism offered by the wargame but limits the analytical power available to the designers. This is especially salient in the case of a pseudo-experimental design where granting players the freedom to act limits the ability to imposed controls and treatments.

Ultimately, one cannot say that one approach is better than the other. Design considerations and objectives should drive the decision of whether or not to grant players the freedom of action within the simulated environment. Furthermore, should designers opt to adopt an experimental approach, the game design ought not to be compromised in order to force aspects of a preferred method into a construct not wholly suited to it.

With respect specifically to understanding decision-making behavior within an uncertain environment, providing participants with the freedom of action contributes significantly to increasing the level of realism. As in the real-world where interpreting adversarial behavior is a daunting task, free-play is the best solution to mimic this salient characteristic. This, in turn, should prompt participants to resort to the equivalent cognitive mechanisms

---

[68] Peter P. Perla and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No. 3, Summer 2011, pp.111-130.

to reduce the degree of uncertainty and thus result in behavior comparable to that in the real world.

F. Cyber-Specific or Cyber-Adjunctive Environment

While being the only aspect directly associated with running a wargame about the cyber domain, the extent to which cyberspace is manifested in the game should be taken into consideration. Tempting as it may be to present a wargame that focuses exclusively on interactions within this domain, most real-world cases are cross-domain in nature. As noted by a growing number of authors, cyberspace is an adjunctive instrument of foreign policy is serves as one of the expressions of national power.[69] With that being said, the extent to which cyber capabilities feature in wargames is a direct reflection of the activity's realism that, in turn, interacts with other aspects of game design such as participant backgrounds. Elites that have experience with real-world cases may find wargames that unfold solely in cyberspace or involve exclusively cyber events unrealistic. Consequently, their actions during the activity may not align with how they would respond under normal circumstances.

This is not to say, however, that there is no merit to running wargames that unfold solely within the cyber domain. Designers are more than welcome to do so as long they bear in mind that decision-making behavior may reflect differently depending on the extent to which participants are exposed to this uncertain environment and their ability to address this uncertainty.

---

[69] Benjamin Jensen, Ryan C. Maness, and Brandon Valeriano, "Cyber Victory: The Efficacy of Cyber Coercion," presented at the Annual International Studies Association Meeting (Atlanta, Georgia, March 17, 2016); Jon R. Lindsay and Erik Gartzke, "Cross-domain deterrence as a practical problem and a theoretical concept," Erik Gartzke and Jon R. Lindsay, eds., Cross-Domain Deterrence: Strategy in an Era of Complexity, (La Jolla, CA: Manuscript, 2016).

VI. Conclusions

Wargames are an under-utilized and under-realized instrument with which both scholars and defense planners might better understand the operational-level pathologies of operation in the fifth domain. The recent turn in cyber conflict studies towards the use of experiments has successfully illustrated the degree to which focus on dynamics at the levels of analysis traditionally found in international relations (IR) scholarship falls short of producing knowledge that can inform policy. Likewise, the increasing tendency to characterize cyber conflict neither as warfighting nor as isolated incidents uncoupled from the broader strategic context of adversary campaigns of contestation supports the notion that one-off findings in research must be corroborated and replicated in diverse methodological applications. Simulations, both simple and complex, are ideally positioned to help researchers answer these imperatives.

Perhaps the most particular point in support of increased use of wargames both in research and in operations planning and training is the utility of the simulation for calibrating what some have called “nano-second” manifestations of policy. In interpreting strategy documentation, operators, investigators, and policymakers alike must build procedures conducive to the effective exercise of cyber conflict response actions. Given that such procedures must effectively highlight and incentivize appropriate reactive options in relatively short time frames, additional efforts must continuously be made to ensure congruence with high-level strategy and doctrine.

With the 2018 promulgation of American cyber policy as now built around the concept of persistent engagement, this reconciliation imperative is stronger than ever. Where the purpose of constant interaction via both preemptive and reactive “defending forward” activities is intended to force the development of mutual understandings of conflict parameters with adversaries, there is a distinct need to simulate and test assumptions about how foreign powers might interpret the actions of the U.S. and her close

partners on a repeating basis. After all, the artificiality of the domain and how cyber engagements take on meaning from real-world corollaries of digital conflict means that defense planners should be unwilling to assume that such interpretations will remain constant over time.

Bibliography

Axelrod, Robert, "A Repertory of Cyber Analogies," in Emily O. Goldman and John Arquilla, eds, *Cyber Analogies* (Monterey, CA: Dept. of Defense Information Operations Center for Research, 2014).

Borghard, Erica D. and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3, May 2017, pp.452-481.

Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2017).

Bumiller, Elisabeth and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

CCDCOE, "Locked Shields 2019," CCDCOE, https://ccdcoe.org/exercises/locked-shields/.

Dean, Benjamin and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy," *Penn State Journal of Law & International Affairs*, Vol. 5, No. 1, April 2017, pp.29-71.

Dunn Cavelty, Myriam, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, Vol. 15, No. 1, January 2013, pp.105-122.

Fearon, James D., "Rationalist Explanations for War," *International Organization*, Vol. 49, No. 3, Summer 1995, pp.379-414.

Finn, Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic, " *The Washington Post*, Last Modified May 17, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

Fischerkeller, Michael P. and Richard J. Harknett, "Persistent Engagement

and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

Gartzke, Erik and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity*, Vol. 3, No. 1, March 2017, pp.37-48.

Gerrig, Richard, *Experiencing Narrative Worlds* (New York: Routledge, 2018).（Ebook）

Gomez, Miguel Alberto, "Past behavior and future judgements: seizing and freezing in response to cyber operations," *Journal of Cybersecurity*, Vol. 5, No.1, September 2019, pp.1-19.

Gomez, Miguel Alberto, "Sound the alarm! Updating beliefs and degradative cyber operations," *European Journal of International Security*, Vol. 4, No. 2, June 2019, pp.190-208.

Gomez, Miguel Alberto and Eula Bianca Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats," *Politics and Governance*, Vol. 6, No. 2, June 2018, pp.61-72.

Gomez, Miguel Alberto and Christopher Whyte, 2019.

Gray, Colin S., *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013).

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, Vol. 3, No. 1, March 2017, pp.49-58.

Hafner-Burton, Emilie M., Alex D. Hughes, and David G. Victor, "The Cognitive Revolution and the Political Psychology of Elite Decision Making," *Perspectives on Politics*, Vol. 11, No. 2, June 2013, pp.368-386.

Hansen, Lene, and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4, December 2009, pp.1155-1175.

Holland, Norman N., "Spider-Man? Sure! The neuroscience of suspending disbelief," *Interdisciplinary Science Reviews*, Vol. 33, No. 4, December 2008, pp.312-320.

Holsti, Ole R., "The Belief System and National Images: A Case Study," *The Journal of Conflict Resolution*, Vol. 6, No. 3, September 1962, pp.244-252.

Holsti, Ole R., "Cognitive Dynamics and Images of the Enemy," *Journal of International Affairs*, Vol. 21, No. 1, 1967, pp.16-39.

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting, "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat," *European Journal of International Security*, Vol. 2, No. 1, February 2017, pp.64-87.

Jensen, Benjamin, Ryan C. Maness, and Brandon Valeriano, "Cyber Victory: The Efficacy of Cyber Coercion," presented at the Annual International Studies Association Meeting (Atlanta, Georgia, March 17, 2016).

Jensen, Benjamin and Brandon Valeriano, "The Cyber Character of Crisis Escala," presented at the International Studies Association Annual Convention (Toronto, March 27, 2019).

Jervis, Robert, *Perception and misperception in international politics*. New edition. ed. (Princeton, NJ.: Princeton University Press, 1976).

Jervis, Robert, "Understanding beliefs and threat inflation," in Trevor A. Thrall and Jane K. Creamer, eds. *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11,* (Abingdon-on-Thames, UK: Routledge, 2009).

Johnson, Dominic and Dominic Tierney, "The Rubicon theory of war: how

the path to conflict reaches the point of no return," *International Security*, Vol. 36, No. 1, Summer 2011, pp.7-40.

Johnson, Dominic and Dominic Tierney, "Bad World: The Negativity Bias in International Politics," *International Security*, Vol. 43, No. 3, February 2019, pp.96-140.

Kahneman, Daniel, "A perspective on judgment and choice - Mapping bounded rationality," *American Psychologist*, Vol. 58, No. 9, September 2003, pp.697-720.

Kahneman, Daniel, *Thinking, fast and slow.* 1st ed. (New York: Farrar, Straus and Giroux, 2011).

Kahneman, Daniel, Paul Slovic, and Amos Tversky, *Judgment under uncertainty: heuristics and biases* (New York : Cambridge University Press, 1982).

Kertzer, Joshua D. and Kathleen M. McGraw, "Folk Realism: Testing the Microfoundations of Realism in Ordinary Citizens," *International Studies Quarterly*, Vol. 56, No. 2, June 2012, pp.245-258.

Khong, Yuen Foong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ.: Princeton University Press, 1992).

Kostyuk, Nadiya and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *The Journal of Conflict Resolution*, Vol. 63, No. 2, February 2019, pp.317-347.

Kruglanski, Arie W. and Donna M. Webster, "Motivated closing of the mind: "Seizing" and "freezing"," *Psychological Review*, Vol. 103, No. 2, April 1996, pp.263-283.

Kunda, Ziva, "The case for motivated reasoning," *Psychological Bulletin*, Vol. 108, No. 3, December 1990, pp.480-498.

Larson, Deborah Welch, "The Role of Belief Systems and Schemas in Foreign Policy Decision-Making," *Political Psychology*, Vol. 15, No.1, March 1994, pp.17-33.

Lau, Richard, R. and David P. Redlawsk, "Advantages and Disadvantages of Cognitive Heuristics in Political Decision Making," *American Journal of Political Science*, Vol. 45, No. 4, October 2001, pp.951-971.

Libicki, Martin C., *Cyberdeterrence and cyberwar* (Santa Monica, CA.: Rand Corporation, 2009).

Liff, Adam, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war," *Journal of Strategic Studies*, Vol. 35, No. 3, June 2012, pp.401-428.

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3, July 2013, pp.365-404.

Lindsay, Jon R. and Erik Gartzke, "Cross-domain deterrence as a practical problem and a theoretical concept," Erik Gartzke and Jon R. Lindsay, eds, Cross-Domain Deterrence: Strategy in an Era of Complexity, (La Jolla, CA: Manuscript, 2016).

Maness, Ryan C. and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society*, Vol. 42, No. 2, April 2016, pp.301-323.

Mintz, Alex, Steven B. Redd, and Arnold Vedlitz, "Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations?" *The Journal of Conflict Resolution*, Vol. 50, No. 5, October 2006, pp.757-776.

Mintz, Alez, and Carly Wayne, "The Polythink Syndrome and Elite Group Decision-Making," *Political Psychology*, Vol. 37, No. S1, February 2016, pp.3-21.

O'toole, Tara, Mair Michael, and Thomas V. Inglesby, "Shining light on "Dark Winter"," *Clinical Infectious Diseases*, Vol. 34, No. 7, April 2002, pp.972-983.

Perla, Peter P. and ED McGrady, "Why wargaming works," *Naval War College Review*, Vol. 64, No. 3, Summer 2011, pp.111-130.

Perrow, Charles, *Normal accidents: living with high-risk technologies Princeton paperbacks* (Princeton, NJ.: Princeton University Press, 1984).

Power, Richard, "The Solar Sunrise Case: Mak, Stimpy, and Analyzer Give the DoD a Run for Its Money," *informit*, October 30, 2000, http://www.informit.com/articles/article.aspx?p=19603&seqNum=4.

Rascagneres, Paul and Martin Lee, "Who Wasn't Responsible for Olympic Destroyer?" Talos Intelligence, February 26, 2018, https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html.

Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp.5-32.

Saltzman, Ilai, "Cyber posturing and the offense-defense balance," *Contemporary Security Policy*, Vol. 34, No. 1, March 2013, pp.40-63.

Saunders, Elizabeth N., "No Substitute for Experience: Presidents, Advisers, and Information in Group Decision Making," *International Organization,* Vol. 71, No. S1, April 2017, pp.219-247.

Schneider, Jacquelyn, 2017.

Schneider, Jacquelyn, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Slayton, Rebecca, "What Is the Cyber Offense-Defense Balance?

Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3, January 2017, pp.72-109.

Slovic, Paul, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "The Affect Heuristic," *European Journal of Operational Research*, Vol. 177, No. 3, March 2007, pp.1333-1352.

USA. "National Cyber Security Strategy of the United States of America," 2018.

USGOV. 2007a. "Estonia's Bronze Soldier: It's Deja Vu All Over Again," WikiLeaks, Last Modified 16.02.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN106_a.html.

USGOV. 2007b. "Estonia's Cyber Attacks: World's First Virtual Attack Against Nation State," WikiLeaks, Last Modified 04.06.2007, accessed 13.06. https://wikileaks.org/plusd/cables/07TALLINN366_a.html.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

Valeriano, Brandon and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research*, Vol. 51, No. 3, May 2014, pp.347-360.

Valeriano, Brandon and Ryan C. Maness, *Cyber war versus cyber realities : cyber conflict in the international system* (New York: Oxford University Press, 2015).

Whalen, Paul J., "Fear, Vigilance, and Ambiguity: Initial Neuroimaging Studies of the Human Amygdala," *Current Directions in Psychological Science,* Vol. 7, No. 6, December 1998, pp.177-188.

Whyte, Christopher, "Ending cyber coercion: Computer network attack, exploitation and the case of North Korea," *Comparative Strategy*, Vol. 35, No. 2, March 2016, pp.93-102.