Game Lab

Connections US Wargaming Conference

National Defense University

July 18th, 2018

"How can we credibly wargame cyber at an unclassified level?"

Game Lab Chair

Stephen Downes-Martin

Contributors

Michael Bond, Stephen Downes-Martin, Andreas Haggman, Clayton Hutto, Michael Markowitz, Douglas Samuelson, Joseph Saur

Game Lab Process and Participants

During the Connections Wargaming Conference a small group of interested people gathered for about an hour to discuss the question ***"How can we credibly wargame cyber at an unclassified level?"*** This document is the edited combination of notes contributed by the below participants:

Lt Col Michael Bond
michael.b.bond2.mil@mail.mil
HQ USAF, Wargaming Division A5SW

Dr. Stephen Downes-Martin
stephen.downesmartin@gmail.com
Research Fellow US Naval War College

Andreas Haggman
andreas.haggman.2014@live.rhul.ac.uk
Royal Holloway University of London

Dr. Clayton Hutto
cjhutto@gatech.edu
Georgia Tech Research Institute (GTRI)

Michael Markowitz
markowim@cna.org
CNA

Dr. Doug Samuelson
samuelsondoug@yahoo.com
InfoLogix, Inc.

Joseph Saur
saur@cs.odu.edu
Wargame Consultant

Table of Contents

1 Abstract

A small minority of cyber experts with wargaming and research experience have security clearances. If cyber operations are researched and gamed only at high levels of classification, then we limit our use of the intellectual capital of the United States and Allies and put at risk our ability to gain edge over our adversaries. We must find ways to wargame cyber[1] at the unclassified level while dealing with information security dangers to best use the skills within academia, business and the gaming community. During the Connections US Wargaming Conference 2018 a small group of interested people gathered for about an hour to discuss the question:

"How can we credibly wargame cyber at an unclassified level?"

The group concluded that it is possible to wargame cyber credibly and usefully at the unclassified level and proposed eight methods for doing so. The group also suggested it is first necessary to demonstrate and socialize this idea by gaming the trade-offs between the classification level and the value gained from wargaming cyber.

2 Governing Factors

2.1 Classification

The DoD cannot wargame *specific offensive cyber means* at a low level of classification. The DoD probably cannot wargame generic means or walk-throughs of scenarios at a low level of classification either since this would signal interest in the means and the scenarios themselves are often classified. Academia can however wargame to explore situations and the pros and cons of different generalized capabilities, and industry (other than DoD contractors) is free to wargame what they like at whatever level of commercial confidentiality they choose.[2] A

[1] "Wargaming cyber" and "gaming cyber" are loose terms which group deliberately left as such to encourage divergent thinking and to avoid becoming too specific.

[2] An example of a useful cyber unclassified cyber game about the real world could be Russia in Donbass using publicly available information provided by Russian, proxy and rebel troops ill-disciplined use of social media and cell phones.

particularly useful source of Cyber expertise will be cyber experts within the Government who do not have security clearances.[3]

However, as Doug Samuelson pointed out, an important consideration when gaming at the unclassified level is that the compilation of unclassified elements may make the entire collection retroactively classified. Although this issue is true of any collection of unclassified information, the deliberate effort to wargame a normally highly classified topic at the unclassified level may introduce different pathways for leakage, spillage and breaches than normally considered. This introduces the need to game approaches to security, access and protection to answer questions dealing with the appropriate level of information security. Doug noted that an approach to gaming and modeling cyber scenarios is required that includes the degree of restriction and disruption our C3 system is imposing on our forces without the need to determine the effects in such detail that classification would be required.

The argument that a high level of information security is required because low levels of information security correlates with mission failure and friendly lives lost is specious. Too much information security will slow dissemination of required information to own troops and commanders, lowering the probability of mission success and raising casualties compared to lower levels of information security with faster dissemination to own commanders and troops. There is a "sweet spot" of information security between too little and too much at which the probability of mission success is highest. We need to better understand the trade-off between information security, timeliness of information flow to own commanders and troops, and probability of mission success to better understand how and when to wargame cyber operations at a low level of classification.[4]

---

[3] See for example Dr. Chris Demchak (https://usnwc.edu/Faculty-and-Departments/Directory/Chris-C-Demchak) at the Center for Cyber Conflict Studies, US Naval War College (https://usnwc.edu/Research-and-Wargaming/Research-Centers/Center-for-Cyber-Conflict-Studies), and Andreas Haggman (https://tinyurl.com/krc93no)
for two examples of this kind of resource.

[4] It is worth noting that when a nation makes progress in applying a topic to national security it will often stop publishing on that topic. This can tell others that such progress us being made. Classifying a previously unclassified topic can be an information security flaw.

The existence of the "Cyber Security Challenge",[5] an unclassified open game and set of challenges dealing with cyber sponsored by the UK Government Communications Headquarters[6] not only to recruit but also to tap into talent demonstrates the possibility and value of gaming cyber at the unclassified level.

2.2 Maturity

An argument was made that cyber operations, warfare and technology are still in relative infancy compared to other warfare domains – comparable to the technological sophistication of airplanes and air forces at the start of WWI – and we lack the necessary skills to prevail in cybered conflict. We can see this in the contemporary literature around both subjects and how they evolved.[7] It therefore makes sense to focus our cyber wargaming efforts at a level which recognizes this infancy not only to explore and develop our understanding of cyber and operations but also to develop the talent necessary to gain an edge in using cyber against our adversaries.

2.3 Uncertainty

Planning is fundamental to all military operations, but widely neglected in wargaming. Real cyber operations may require planning long in advance which in itself increases the levels of uncertainty about timing, probability of when and whether it works, nature of the effects, and attribution during cyber operations. We can rarely do cyber "BDA"; when we do see an effect, we don't know for sure what caused it. The characteristics of cyber weapons combined with uncertainties imply a trade-off between reducing different uncertainties, and the need to game policy decisions about funding offensive cyber capabilities versus cyber protection (assuming you can't have it all).

Time flow in a cyber game is a problem. Planning long in advance, the uncertainty of when (and if) a cyber weapon effect occurs after it has been "launched" and the uncertain time

[5] https://www.cybersecuritychallenge.org.uk/

[6] https://www.gchq.gov.uk/

[7] See for example "Curb Your Enthusiasm: Why the Future is Not Stuxnet" by Andreas Haggman in the Proceedings of the 14th European Conference on Cyber Warfare and Security, UK, July 2015, (pp. 397-403).

delays in each side discovering it has been "hacked" after an opponent's offensive launch makes designing the game clock an interesting problem.

2.4 Design

An important first step in wargaming cyber is understanding the purpose and intent of the cyber element of the game, for example education & training, analyzing TTPs, assessing potential impacts of particular techniques on types of targets, teaching policy makers and senior leaders about cyber issues. Although understanding the purpose and intent of any game should always be the first step in game design, the issue of gaming a normally highly classified topic at the no or low levels of classification may introduce new elements of objectives analysis and game design not normally required or present.

Given the lead times involved in developing and planning the use of cyber weapons and defenses and the fact that we are already engaged in pre-kinetic cyber warfare, there's a cyber wargame analogy to Peter Perla's "cycle of research":[8] (1) Cyber pre-game involving policy, investment, research and development -- a "buying game", (2) cyber operational game (combined with kinetic), (3) cyber post-game, then iterate.

Adjudicating any part of a cyber wargame (but specifically the cyber pre-game cyber) is likely difficult given the uncertainties and time leads involved.[9] Perhaps sensitivity analysis around trade-offs is the best way to proceed. This makes it vital to be explicit and transparent with all assumptions.

Just because one is gaming Cyber does not mean that normal wargaming best practices in game design, execution and analysis can be ignored. A number of issues arose during the game lab that must not be forgotten when designing a cyber wargame:

- Red gets to use cyber on us during the game cycle, so we should also wargame options for the architecture of defensive systems.

---

[8] Peter Perla, "The Art of Wargaming", United States Naval Institute 1990

[9] This implies that cyber wargaming is inductive. For more on the differences between inductive and deuctive wargaming see Stephen Downes-Martin, "Adjudication: The Diabolus in Machina of Wargaming", Naval War College Review 2013, Vol 66, No. 3, pp 67 – 80 (http://digital-commons.usnwc.edu/nwc-review/vol66/iss3/6/)

- Red can win at any point of the game cycle.
- Because currently we still need people in charge of the C2 of executing real cyber-attacks game design should limit the number and kind of attacks that are possible during the wargame in a given period.
- The game designer should consider blowback and unanticipated consequences of cyber operations including the effect on us of our offensive cyber operation on them.
- "Wunderwaffen" almost always disappoint in actual combat and the same will be true of cyber weapons, so be ruthless in adjudicating cyber effects.
- Many campaign models include assumptions about having reliable C4ISR from Phase Zero. Disrupting these assets can have critical effects, assessing how much effect and whether it can be mitigated involves knowing what other assets and plans are affected.
- Cyber is large and encompassing; it spans all sectors of critical infrastructure...so Wargaming for cyber may be more than just a military vs military-oriented game. In addition, within military cyber gaming it is important to game holistically combining all the relevant domains. For example, the Center for Army Analysis has SMEs in three electronic domains (EW, Cyber, Space) who discuss capabilities and effects for combinations of these domains, not just each domain independently.

3 Proposed Wargame Methods

3.1 Game the Trade-off between Security and Mission Success

Doug Samuelson suggested gaming and modeling the degree of restriction and disruption our C3 system is imposing on our forces and related institutions, without determining the likely effects in such detail that classification would be required. This can be done in general terms at an unclassified level with informative recommendations for the high side. The topic includes not only the usual protected information, but also excursions and incursions into dark side sites and currency. For example, if government is known not to allow most of its people access to certain classes of sites, those sites can become a very effective venue for bad folks to exchange information and assets. Similarly, over-protection against disinformation could suppress considerable legitimate media activity.

3.2 Develop a Catalog of Effects

Michael Bond proposed developing a catalog or taxonomy of known and possible classes of cyber offensive and defensive actions, assets, target types and vulnerabilities, and effects from open literature. We would want these taxonomies at various echelon scales (tactical, operational, strategic) and on different time scales (many months or even years for strategic

cyber COAs, weeks or months for campaigns COAs, hours or days for tactical COAs). The catalog or taxonomy should contain probabilities of success for each action and possibly mitigating measures. There may be (public) data to support a certain subset of actions in order to populate the values. This all would work toward the credibility and classification.

Andreas Haag warned that a catalogue of "what we know cyber can achieve" (e.g. take out air defenses) only demonstrates what was once achieved – likely those vulnerabilities have been patched, catalogue is a historical artefact, not a guide. It is however a starting position, and like a taxonomy will indicate missing items that are worth investigating and gaming.

3.3 Game the Vulnerabilities Equities Process

Andreas Haag proposed that the Vulnerabilities Equities Process (VEP)[10] is a system which can be turned into a game,[11] and could be a line of research in wargaming cyber. Two people who are knowledgeable about the VEP (and have diverging views) are Katie Moussouris[12] and Dave Aitel[13]. They and/or their published material might be useful resources and a starting point for gamifying the VEP.

3.4 Game the People, not just Things or Secrets

Michael Markowitz pointed out that the key operational cyber asset may be people (skilled operators) not stuff or secrets.[14] So the command level decisions that matter could be the allocation of people to tasks. The flip side of this is that the key operational cyber targets might

---

[10] For more information on the VEP see https://epic.org/privacy/cybersecurity/vep/ and https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[11] "The Timing of Cyber Conflict" by Robert Axelrod and Rumen Iliev (http://www-personal.umich.edu/~axe/Axelrod%20Iliev%20Revised.pdf)

[12] Katie used to work for Microsoft where she set up their bug bounty programme and was also involved in setting up the DoDs 'Hack the Pentagon' programme. See her keynote at CyCon 2017 https://www.youtube.com/watch?v=uogoZQyeDEU.

[13] Dave Aitel is vocal in the information security community. See his blog at https://cybersecpolitics.blogspot.com/.

[14] An example in the commercial world was provided by a bank manager of one of the game lab participants: "85% of our customers out here (Herndon, where many people from three-letter agencies live) mail in their mortgage payments" (to avoid exposure to electronic hacking).

be people (by analogy with hard and soft kinetic targets, contractors in logistics might be an ideal soft cyber target). It may be easier/simpler to target civilian contract labor resources and networks; or other infrastructure sectors. Design of such games need to include system interdependencies and interactions within, between, and among critical infrastructure sectors.

A game addressing cyber targeting of people doesn't have to involve details about physical systems and assets that would raise classification (although representing specific people or specific agency roles in a game might be problematic – in which case use generalized characteristics of people and agencies).

3.5 Use Techniques from the Hobby Game World

Michael Markowitz suggested hobby wargaming as a source of techniques for cyber gaming at the unclassified level.[15] For example, use two card decks:

1. effects and
2. multiple probability options

and then use dice modifiers +/0 column shifts to focus on the effect cyber operations has on modifying force effectiveness without delving into the characteristics of specific cyber weapons and their targets. He noted two games from the hobby world that are worth examining for techniques relevant to gaming cyber; "Plot to Assassinate Hitler"[16] is a game of two networks trying to penetrate and subvert each other, and "Bodyguard Overlord"[17] is a simulation of intelligence and deception and the effects on military operations.

Andreas Haggman proposed that to deal with the immature level of our understanding of how to use cyber in conflict and to increase the level of cyber skills in our warfighting services, we should develop hobby games that deal with cyber in an analogous way the game "Ace of Aces" deals with air power (in its infancy). Ace of Aces wonderfully captures both the basics and

[15] And not just board game mechanics, but also design principles come out of the unclassified hobby gaming world. See for example "Designing Cyber Wargames" by Roger Mason, July 12 2018, https://www.lecmgt.com/blog/designing-cyber-wargames/.

[16] Designed by Jim Dunnigan and published in in 1976 by Strategy & Tactics magazine #59 (https://boardgamegeek.com/boardgame/3575/plot-assassinate-hitler)

[17] Designed by John Prados and published in 1994 by Spearhead Games (https://boardgamegeek.com/boardgame/4010/bodyguard-overlord)

intricacies of air combat (at the tactical level, and at the maturity level of WWI) without getting bogged down in the technology itself.[18] We need a "Hack of Hackers" type game to generate interest for recruitment purposes, teach terminology, and explore the domain admittedly at a higher level of complexity and breadth than the very focused "Ace of Aces". An example of a commercial unclassified game that teaches cyber topics is [d0xed!][19] and can perhaps be used to inspire a more operational multi-sided game dealing with cyber at the unclassified level.

3.6 Use Unclassified Games Sponsored by Governments

Stephen Downes-Martin suggested that games such as the UK Government sponsored unclassified "Cyber Security Challenge" provide a starting point for developing unclassified cyber wargames for research and identification and recruitment of talent. Identifying other open gaming systems sponsored by other governments and agencies is a potentially valuable activity. When combined with MMOGs these might provide very interesting insights into cyber operations and effects in the economic and political arenas. The approach taken by the US Navy with its MMOWGLI system[20] could be adapted for cyber operations for example.

3.7 Game the Generalized Characteristics of Cyber, not the Specifics

Stephen Downes-Martin proposed that a possible approach to researching and wargaming cyber at an unclassified or low level of classification is to focus on the generalized characteristics and effects of cyber and information weapons independent of the detailed characteristics of specific cyber weapons. One can usefully research and explore the effects and wargame the operational usefulness of characteristics of a kinetic weapon without having to use the classified details of a specific example of that weapon. Similarly, it may be useful to wargame the usefulness of generalized cyber capabilities to explore the possible operational value and dangers of those capabilities and of the relationships and trade-offs between those characteristics.

---

[18] https://boardgamegeek.com/geeklist/1570/ace-aces-picture-book-game-system

[19] For a description of [d0xed!] and to download the game go to http://d0x3d.com/d0x3d/welcome.html.

[20] MMOWGLI – "Massive Multiplayer Online Wargame Leveraging the Internet, enables collaborative thinking and innovation. Players build Ideas and Action Plans together on the Web" https://portal.mmowgli.nps.edu/game-wiki

For cyber however the characteristics may look very different, and it is these differences that are interesting. For example, artillery rounds remain effective no matter how many have been fired in the past. Their trajectory, time on target and point of impact (CEP), weight and effects are important considerations and are determined by well understood physics. The equivalent characteristics of cyber weapons are very different. They often become ineffective after first use (the adversary can make themselves invulnerable to them), their trajectory through cyberspace (the internet) is unknown (raising interesting political issues), time to become effective and the effect itself are highly uncertain, and collateral damage may be uncontrollable. Nevertheless, wargaming weapons with these general and unclassified characteristics is possible and valuable for tactical, operational, strategic and planners.

3.8 Game STRATPOL Cyber, not just Military

Stephen Downes-Martin noted that awareness is growing in the political space about the (successful?) attempts of our adversaries to subvert our democratic and commercial/economic processes (and hence our national security) by attacking the belief systems of our populations and senior leaders. This is a form of cyber warfare with potentially strategic and operational level warfare implications and a large amount of data on the subject is in the public domain. We can and should wargame "offensive knowledge warfare" enabled by cyber and aimed at the general population at the unclassified level.[21]

[21] Stephen Downes-Martin, "Offensive Strategic Knowledge Warfare in the Shared Cyber Domain", Stephen Downes-Martin, Operationalizing Cyber Strategies Workshop, US Naval War College, May 3, 2012, (https://tinyurl.com/y94bf9pa)

4 Conclusions and Recommendations

First one must demonstrate and socialize the idea that it is possible to wargame cyber usefully and credibly at the unclassified level. One does this by gaming the trade-offs between security, access, and information protection versus the value gained from gaming cyber. Then research and explore wargaming cyber at the unclassified level using a mix of the following approaches:

1. Game the degree of restriction and disruption our C3 system is imposing on our forces and related institutions
2. Develop a taxonomy or catalog of unclassified effects
3. Game the Vulnerabilities Equities Process
4. Focus on targeting people and social engineering
5. Use techniques from the hobby world
6. Use Unclassified Games Sponsored by Governments such as the UK Government "Cyber Security Challenge" and the US Navy MMOWGLI
7. Focus on the characteristics of cyber weapons and how these differ from the analogous characteristics of kinetic weapons
8. Game strategic, political and economic cyber

and embed in a cyber "cycle of gaming":

- "buying pre-game" input from Perla's cycle of research
- cyber wargame including kinetic
- post-game analysis and output back into Perla's cycle of research
- iterate