

THE CYBER DEFENSE REVIEW

International Conference on Cyber Conflict (CyCon U.S.)

November 18-20, 2019

Defending Forward



♦ POLICY PAPERS ♦

A Framework of Partnership

Dr. Jim Chen

Civilians 'Defending Forward' in
Cyberspace: Aligning Cyber Strategy
and Cyber Operations

Dr. Matthew J. Flynn

Norms and Normalization

Dr. Martin C. Libicki

Operational Decision-Making
for Cyber Operations:
In Search of a Model

Dr. Max Smeets
JD Work

♦ TECHNICAL PAPERS ♦

Overview of 5G Security
and Vulnerabilities

Shane Fonyi

A Quest for Indicators of Security Debt

Simo Huopio

Wargaming and the Education Gap:
Why *Cyber War: 2025* Was Created

David Tyler Long

The Cyber Defense Review:
CyCon U.S. 2019 Conference Papers

Colonel Andrew O. Hall

THE CYBER DEFENSE REVIEW

◆ SPRING EDITION ◆

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

EDITOR IN CHIEF

Dr. Corvin J. Connolly

MANAGING EDITOR

Dr. Jan Kallberg

DIGITAL EDITOR

Mr. Tony Rosa

AREA EDITORS

Military Operations

Col. Paul Goethals, Ph.D.
Maj. Charlie Lewis

Machine Learning

Dr. Steve Henderson
Dr. Fernando Maymi
Sgt. Maj. Jeffrey Morris, Ph.D.

Information Theory

Dr. David Thomson

Social Threat Intelligence

Ms. Elizabeth Oren
Dr. Paulo Shakarian

National Security

Dr. Chris Bronk
Dr. David Gioe

Network Security

Dr. Michael Grimaila
Lt. Col. William Clay Moody, Ph.D.
Dr. David Raymond

Computational Modeling

Dr. Robert Thomson

Human Factors

Lt. Col Erica Mitchell

Law and Ethics

Prof. Robert Barnsby, J.D.
Lt. Col Mark Visger, J.D.

Data Science

Dr. Harold J. Arata III
Maj. Nathaniel D. Bastian, Ph.D.
Dr. Dawn Dunkerley Goss

International Relations

Dr. Aaron Brantly
Ms. Elsa Kania

EDITORIAL BOARD

Col. Andrew O. Hall, Ph.D. (Chair.)

U.S. Military Academy

Dr. Amy Apon

Clemson University

Dr. Chris Arney

U.S. Military Academy

Dr. David Brumley

Carnegie Mellon University

Dr. Martin Libicki

U.S. Naval Academy

Ms. Merle Maigre

CybExer Technologies

Dr. Michele L. Malvesti

Financial Integrity Network

Dr. Milton Mueller

Georgia Tech School of Public Policy

Dr. Hy S. Rothstein

Naval Postgraduate School

Dr. Bhavani Thuraisingham

The University of Texas at Dallas

Ms. Liis Vihul

Cyber Law International

Prof. Tim Watson

University of Warwick, UK

CREATIVE DIRECTORS

Sergio Analco

Gina Daschbach

LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

PUBLIC AFFAIRS OFFICER

Capt. Lisa Beum

KEY CONTRIBUTORS

Clare Blackmon

Nataliya Brantly

Kate Brown

Erik Dean

Martha Espinoza

Shane Fonyi

Col. John Giordano

Lance Latimer

Eric Luke

Alfred Pacenza

Diane Peluso

Michelle Marie Wallace

CONTACT

Army Cyber Institute

Spellman Hall

2101 New South Post Road

West Point, New York 10996

SUBMISSIONS

The Cyber Defense Review

welcomes submissions at

mc04.manuscriptcentral.com/cyberdr

WEBSITE

cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

© U.S. copyright protection is not available for works of the United States Government. However, the authors of specific content published in The Cyber Defense Review retain copyright to their individual works, so long as those works were not written by United States Government personnel (military or civilian) as part of their official duties. Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.

The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

CONFERENCE PROFILE

2019 International Conference on Cyber Conflict U.S. (CyCon U.S.)

November 18th, 2019 - November 20th, 2019

Crystal Gateway Marriott

Alexandria, VA

INTRODUCTION

COLONEL ANDREW O. HALL	9	CyCon U.S. 2019 Conference Papers
-------------------------------	---	-----------------------------------

POLICY PAPERS

DR. JIM Q. CHEN	15	A Framework of Partnership
------------------------	----	----------------------------

DR. MATTHEW J. FLYNN	29	Civilians ‘Defending Forward’ in Cyberspace: Aligning Cyber Strategy and Cyber Operations
-----------------------------	----	---

DR. MARTIN C. LIBICKI	41	Norms and Normalization
------------------------------	----	-------------------------

ALAN MEARS JOE MARIANI	55	The Temporal Dimension of Defending Forward: A UK perspective on how to organize and innovate to achieve US Cyber Command’s new vision
-----------------------------------	----	--

DR. JAMES E. PLATTE	75	Defending Forward on the Korean Peninsula: Cyber Deterrence in the U.S.-ROK Alliance
----------------------------	----	--

DR. MAX SMEETS JD WORK	95	Operational Decision-Making for Cyber Operations: In search of a model
-----------------------------------	----	--

TECHNICAL PAPERS

SHANE FONZI	117	Overview of 5G Security and Vulnerabilities
SETH T. HAMMAN JELENA VIČIĆ JACK MEWHIRTER PHILIP WHITE RICHARD J. HARKNETT	135	Deciphering Cyber Operations: The use of methods and simulations for studying militarystrategic concepts in cyberspace
FORREST HARE WILLIAM DIEHL	153	Noisy Operations on the Silent Battlefield: Preparing for adversary use of unintrusive precision cyber weapons
SIMO HUOPIO	169	A Quest for Indicators of Security Debt
DAVID TYLER LONG	185	Wargaming and the Education Gap: Why <i>CyberWar: 2025</i> Was Created

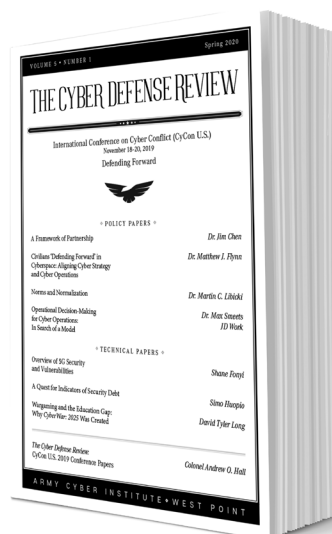
THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

VOL. 5 ♦ NO. 1

The Cyber Defense Review: CyCon U.S. 2019 Conference Papers

Colonel Andrew O. Hall
Director, Army Cyber Institute
United States Military Academy



INTRODUCTION

Welcome to the Spring edition of *The Cyber Defense Review* (CDR), and the exciting publication of the CyCon U.S. 2019 conference papers. This edition of the CDR will feature 6 policy and 5 technical papers that dramatically provide texture and insight into the complicated Defending Forward strategy. The 11 papers were presented on November 18-20, at the Crystal Gateway Marriott in Alexandria, VA. The CyCon U.S. conference is the premier forum on cyber conflict. It is a collaborative effort between the Army Cyber Institute (ACI) at West Point and the NATO Cooperative Cyber Defence Centre of Excellence and complements the CyCon Conference held every spring in Estonia.

The CyCon U.S. conference theme was Defending Forward and followed the Department of Defense's (DoD) 2018 Cyber Strategy, which identified the need for active preparedness in cyberspace by "defending forward." This strategy intends to disrupt or halt malicious cyber activity at its source, and degrade said activity before it can reach its intended victim. The "defending forward" strategy engages the private sector as a pivotal ally in defending the nation's networks.

The 2019 conference was an immense success that was attended by 337 people from over 40 companies, 13 universities, 17 foreign nations, congressional staffers, and various government organizations. A post-event survey found that 92% of respondents reported the topics as being useful to their work, 93% thought that the event advanced the cyber body of knowledge, and 100% believed that it succeeded in creating or maintaining productive partnerships. Videos of the panels and speakers are posted on the ACI's website to allow a wider audience to access this valuable information: <https://cyber.army.mil/>. We thank all those who submitted papers, attended the conference, and worked so diligently behind the scenes to make this a spectacular event.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Colonel Andrew O. Hall is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, Colonel Hall leads a 70-person, multi-disciplinary research institute and serves as the Chairman of the Editorial Board for *The Cyber Defense Review* (CDR) journal; and Conference Co-Chair for the International Conference on Cyber Conflict U.S. (CyCon U.S.). He has a B.S. in Computer Science from the USMA, an M.S. in Applied Mathematics from the Naval Postgraduate School, and a Ph.D. in Management Science from the University of Maryland. Colonel Hall additionally teaches in the Department of Mathematical Sciences and the Department of Electrical Engineering and Computer Science at the USMA. Since 1997, Colonel Hall's military career has been focused on operations research and solving the Army's most challenging problems using advanced analytic methods. Colonel Hall also serves as the President of the Military Applications Society of the Institute for Operations Research and the Management Sciences. His research interests include Military Operations Research, Cyber Education, Manpower Planning, and Mathematical Finance.

The CyCon U.S. conference committee selected 11 peer-reviewed scholarly papers for presentation at the conference from the 40 papers submitted for consideration (a 27% selection rate). These papers were presented at CyCon U.S. under the following two session topics: Policy and Technical. Following publication in the Spring CDR, the papers will be indexed in JSTOR for access by other cyber researchers.

The Spring CDR begins with the Policy papers and Dr. Jim Chen's "A Framework of Partnership Methods." He contends that cyberspace requires a partnership between the public and private sectors. Dr. Chen recommends a whole-of-society approach due to the holistic nature of cyber threats. The second article of the Spring CDR is Dr. Matthew Flynn's "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operation," which advocates for a new US military cyber strategy that relies on increased civilian involvement. In "Norms and Normalization," Dr. Martin Libicki brilliantly examines nation-state cyber activities and *de facto* norms in cyberspace. The fourth policy article is Alan Mears and Joe Mariani's "The Temporal Dimension of Defending Forward," which tackles U.S. Cyber Command policy from a UK perspective. Next up is "Defending Forward on the Korean Peninsula," by Dr. James Platte of the U.S. Air Force Center for Strategic Deterrence Studies (CSDS). He examines cyber deterrence in the Korean AOR as part of the overall strategic deterrence posture of the U.S.-ROK alliance. The Policy section ends with Dr. Max Smeets and JD Work's captivating study "Operational Decision-Making for Cyber Operations: In Search of a Model." Their work explores the complexity of cyber operations and the decision dynamics of cyber conflict.

Our CDR readers will thoroughly enjoy all five Technical papers. Shane Fonyi from the ACI crafts a superb and timely work that covers the 5G security space, technologies, and vulnerabilities in "Overview of 5G

Security and Vulnerabilities.” Seth T. Hamman, Jelena Vičić, Jack Mewhirter, Philip White, and Richard J. Harknett collaborate on “Deciphering Cyber Operations: The Use of Methods and Simulations for Studying Military Strategic Concepts in Cyberspace.” They brilliantly describe a simulation framework to study the dynamics of cyber operations below the threshold of armed attack. Forrest Hare and William Diehl’s, “Noisy Operations on the Silent Battlefield” provide examples of non-intrusive precision cyber weapons used in real-world operations. Simo Huopio from the Finnish Defence Research Agency examines Technical Debt (TD) and offers an innovative solution framework in “A Quest for Indicators of Security Debt.” The last article in this Spring Edition is David Tyler Long’s “The Cyberspace Operations Wargaming and Education Gap,” which highlights the importance of wargaming to the development of sound cyber policy and doctrine.

The next CDR will be our first themed edition and will focus on Information Operations (IO). Daily, our competitors are leveraging IO to influence what we believe, while intending to sow distrust and impact how we behave. IO is now a joint warfighting function, and the US military is focused on preparing to compete in Information Warfare (IW) to win future conflicts. We are honored to showcase articles from LTG Stephen Fogarty, Lt Gen Timothy Haugh, BG (Ret.) Jeff Smith, Dr. Martin Libicki, Bryan Sparling, Tim Thomas, Dr. Herb Lin, Dr. Chris Paul, and Renny Gleeson. This thought-provoking themed edition will explore the differences between IO and IW, tackles the media’s role in IO, and analyze our adversaries’ IO strategy during competition, pre-crisis, and conflict.

Please check our Call for Papers announcement on the CDR website to submit articles on “Cyber Economics” for a themed Spring 2021 CDR: <https://cyberdefensereview.army.mil/>. This issue will explore cyber’s impact on the US economy, the data behind cyber economics, the cyber risk management, the monetary value of cyber incidents, the economics of national cyber strategy, and leadership and business decision-making. We welcome a multidisciplinary and international examination of this vital topic. I encourage our readers to submit cyber economic research papers, commentaries, research notes, and book reviews on the CDR *ScholarOne* platform: <https://mc04.manuscriptcentral.com/cyberdr>.

I want to recognize the extraordinary talent and creativity of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, and Courtney Gordon-Tennant for transforming this signature edition. Please enjoy these thoughtful papers, and may their relevance guide our continued cyber conversation together! ♥

THE CYBER DEFENSE REVIEW

◆ POLICY PAPERS ◆

A Framework of Partnership

Professor Jim Q. Chen, Ph.D.

ABSTRACT

The persistent engagement strategy in cyberspace requires partnership between the public and private sectors. This whole-of-society approach is greatly needed, as cyber threats are holistic. Partnership can yield a number of good outcomes that all parties seek to achieve. However, having truly productive partnership requires a significant amount of time and effort. There are different partnership methods that ask for different amount of time, effort, and resources. Hence, it is crucial to have a better understanding of the requirements of each partnership method. To this end, this article proposes a framework that incorporates various partnership methods with aims to achieve various goals. It demonstrates that this framework can provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements.

I. INTRODUCTION

In an interview with the *Joint Force Quarterly*, U.S. Cyber Command Commander General Paul Nakasone^[1] emphasizes the importance of partnership in persistent engagement strategy. He states that “enabling our partners is two-thirds of persistent engagement. The other third rests with our ability to act – that is, how we act against our adversaries in cyberspace. Acting includes defending forward.” Likewise, U.S. Presidential Policy Directive 41 (PPD-41)^[2] specifically addresses coordination in dealing with cyber incidents, especially coordination between and among federal agencies as well as coordination between the public and private sectors. It directs inclusion of critical private-sector stakeholders within Cyber Unified Coordination Groups (UCG) when significant cyber incidents occur.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Without a doubt, partnership effort is needed for successful cyber defense, including forward defense, because cyber threats are threats to the society as a whole. Victims of cyber attacks range from government agencies to private companies and individual citizens. In order to disrupt or halt malicious cyber activity at its source and degrade said activity before it can reach its intended victim, all relevant parties should be engaged. This common defense calls for partnership across all sectors of society, but especially between the government and the private sector. The efforts from the government and the private sector are complementary. No effort from any party will lead to the failure of the overall defense.

Partnership, especially partnership between the government and the private sector, is the key to enhance capability and provide resilience in cyber defense. However, it is always a challenge to establish and maintain partnership because partnership is built on trust, which requires time. The unique relationship between the two sides also needs to be maintained. Both sides should “give” in order to “take,” as partnership ought to have proportional investment from both sides. Before entering into a partnership relationship, both sides should have a clear understanding of the types of methods and the relevant effort required. In this way, both sides know what is expected in this relationship. As a matter of fact, there is no structured guidance to nurture such an effort. This article attempts to bridge this gap by proposing a framework that incorporates various partnership methods between the government and the private sector. It assumes that these methods sit on varied points of a partnership spectrum to support varied goals. This framework helps to address the following questions: What are the different types of partnership methods? What is involved in each method? How can an effective partnership between the government and the private sector be developed? Ultimately, this framework provides guidance for the selection of an appropriate partnership method in a specific environment. The guidance provided is based on specific conditions, needs, and requirements.

In the following sections, an analysis is performed, revealing what is missing in the current approach to partnership. Then, a framework that consists of a spectrum of various partnership methods such as cooperation, collaboration, and integration is proposed. The advantages of this new approach are discussed, and future research is also recommended.

2. ISSUES

The public-private partnership has been a cornerstone in the U.S. national cybersecurity strategy for the most recent administrations^[3, 4, 5, 6] as well as in the U.K. national cybersecurity strategy^[7]. As mentioned by Carr^[8], the public-private partnership has also been included in national cybersecurity strategies in many other countries in the world. This shows the importance of the public-private partnership and the emphasis that many governments have placed on it.

There are several reasons for the promotion of the public-private partnership. At least the following three reasons have to be mentioned: (1) Critical infrastructure is mainly owned, managed, and operated by the private sector in the U.S. and in some other countries. In an

environment like this, the government has to work closely with the private sector, i.e. the owners, the managers, and the operators, in order to protect critical infrastructure. U.S. Presidential Policy Directive 21 (PPD-21)^[9] identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems. These sectors are mainly owned, managed, and operated by the private sector. (2) Victims of cyber attacks are from all walks of life. The whole-of-society strategy requires all sectors of society be engaged in cyber defense, both public and private. Absence of one sector may lead to some unexpected consequences. (3) The government may possess specific information on threats and vulnerabilities. Sharing this information with the private sector may help enhance its specific defense posture before real attacks occur. The private sector may also hold some specific pieces of information about attacks for the compromised networks that it owns and manages. Sharing these with the government may help the government gain a comprehensive view of cyber attacks in its country, allowing for effective countermeasures at the national level to be designed and launched. In this respect, the exchange of information may benefit both sectors in enhancing cyber defense posture.

However, it is never an easy task to implement a public-private partnership. As mentioned by Blacker^[10], “national cybersecurity guidance mandates collaboration, but does not speak to (nor should it) how to actually collaborate.” Besides, there are some issues in the current approach to a public-private partnership. These issues are examined below.

First, responsibility and accountability are not clearly defined. As a result, mutual trust is difficult to maintain, and chaos may occur time and again. Without appropriate coordination, one side may accidentally step on the toes of the other side, and both sides may flinch at performing a task at another time. What is worse, both sides may refuse to accept any responsibility when something goes wrong. At the end, it becomes hard to hold anyone accountable, and the partnership may collapse.

Second, the common ends, ways, and means of a partnership are not often considered. Consequently, the partnership becomes aimless. No good strategy is figured out. Neither side knows why, how, or what should be done in order to make the partnership work successfully.

Third, the differences between the two sides are not well considered, not mentioning the different goals that the two sides have. Without reconciling these goals, it is difficult to build a shared work platform. As pointed out by Carr^[11], the government is politically focused, as it is more concerned about the common public good and national security. It employs a hierarchical, or vertical, management structure. However, the private sector is more concerned about profits for enterprises. The private sector has full ownership of enterprises. To achieve its business goals, i.e. to make business efficient and profitable, a horizontal management structure is employed. In Wettenhall^[12]'s term, a horizontal management structure is characterized by

consensual decision-making, while a hierarchical management structure is characterized by having one side in a controlling role.

To summarize, the current approach to the public-private partnership lacks responsibility and accountability; lacks common ends, ways, and means; and lacks effective modes of reconciliation. The issues are associated with “a persistent ambiguity with respect to the parameters of such a partnership,” just as Carr^[13] states. As neither side has a clear view of what should be the give and take, the partnership becomes an ad hoc endeavor. As a consequence, the partnership cannot achieve what it is expected to achieve.

To deal with these issues, the scope of involvement in a partnership should be explicitly defined. In the next section, a framework comprised of various partnership methods is proposed, and each method is explored.

3. A FRAMEWORK OF PARTNERSHIP METHODS

The framework of partnership proposed here should be able to address the three issues discussed above, so that each side knows what is expected of them before it enters into a partnership. The framework consists of a spectrum containing various partnership methods, such as cooperation, collaboration, and integration. Each method is associated with different roles and responsibility as well as ends, ways, and means. The framework helps to understand the give and take of each method.

There exist many partnership methods. Here, in this research, three major ones are focused on. These are: cooperation, collaboration, and integration. These three methods sit on varied points on a partnership spectrum. Within this spectrum, cooperation requires the least effort from both sides, while integration requires the most effort from both sides.

The high-level representation of the spectrum is displayed in Figure 1 below:

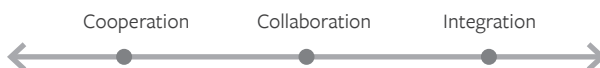


Figure 1. Spectrum of different partnership methods

In a cooperative relationship, a horizontal management structure is maintained. Both sides are independent from each other, even though they have a common task to accomplish. No roles or responsibilities are clearly assigned to relevant team members. No formal procedure is followed. There is no special budget for a task in most cases. Both sides may put resources together whenever needed. The relevant people from both sides work together in an informal environment whenever needed. This relationship is symbolically represented below:



Figure 2. Cooperation

A voluntary, cyber-related, information-reporting mechanism is an example of cooperation. A government agency may acquire a critical piece of information from a private-sector company, which, in return, may receive useful pieces of advice for cyber defense from a government agency. Both sides may benefit from this mechanism, but neither side is in absolute control. Besides, neither side needs to have a big investment for the use of this mechanism.

In a collaborative relationship, a horizontal management structure is maintained. Both sides remain independent from the other while they take on a common task. They select people from both sides to form a special group to work together on a particular task. Both sides are in charge. Roles and responsibilities may or may not be assigned. People from both sides form a group and work together in an informal environment. A special budget may or may not be allocated. Both sides may put resources together whenever needed. This relationship is represented below:

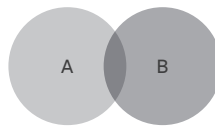


Figure 3. Collaboration

An active threat intelligence-sharing group is an example of collaboration. It involves stakeholders and participants, such as national security agencies, law enforcement agencies, cybersecurity industry companies, non-cybersecurity commercial companies, and other relevant actors. Well-established, cyber-focused, public-private collaboration in current practice includes, but is not limited to, Information Sharing and Analysis Centers (ISACs), automated indicator sharing through Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and the Cyber Information Sharing and Collaboration Program (CISCP). Personnel and resource investment is required to support these efforts, which are beneficial for all stakeholders and participants.

The true public-private collaboration in Healey^[14]'s framework falls into this category, as joint governance is guaranteed and personnel exchange is supported.

In an integrative relationship, one side absorbs the other side into its organization. Now, one side is in total control. A horizontal management structure changes into a hierarchical management structure. Those who work on a task form a special unit of the organization. They work in a formal environment. A formal procedure is followed. A special budget is allocated. Resources are provided. Bureaucracy may be developed in some cases. This relationship is represented below:

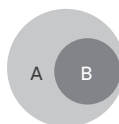


Figure 4. Integration

Having groups of employees from the private sector embedded into a government cyber operation organization as individuals or as new units is an example of integration. In this environment, employees from the private sector have to strictly follow the instruction of the government organization in order to support the mission.

The government-led approach in Healey^[14]'s framework falls into this category as the government maintains the total control. Private-sector employees who join the government efforts are compelled to follow all government policies and regulations. All the maneuvers are orchestrated in order to accomplish missions.

Likewise, the private-led approach in Healey^[14]'s framework also falls into this category. In this environment, one private-sector company is taking the lead. It thus has full control and final say in operations.

Several factors have to be considered when analyzing these partnership methods. One factor is the promotion of trust. Any relationship will not last if there is no mutual trust. Osborne^[15] is an advocate for trust. He maintains that trust can help to develop a "mutual belief in the positive gains of both partners." This belief can serve as the motivation for partnership efforts. Manley^[16] echoes the same view. He takes one step further and makes trust the foundational level for his proposed public-private partnership model.

Another factor is the assignment of responsibility. If specific roles and responsibilities are not assigned to relevant people, the leadership of a group cannot be empowered; communication within the group cannot be enhanced; relationships inside the group cannot be improved; reliability cannot be guaranteed; and accountability cannot be assured when something goes wrong.

Still another factor is the employment of checks and balances. If a task is led by one entity, checks and balances are seldom conducted. However, if it is led by two entities, while one entity performs the task, the other entity can play the role of checks and balances. These roles are interchangeable while the function of checks and balances is still maintained. Meanwhile, transparency and due process or fairness should be guaranteed.

In Eichensehr^[17]'s assertion, without "accountability, transparency, and due process or fairness," the partnership effort will fall short of "public law values."

One more factor is the adoption of the bottom-up approach, which encourages voluntary partnership and should be utilized. It is the opposite of the top-down approach. As pointed out by Osborne^[15], the top-down approach, which is the "rigid set of formal partnership" set up on strict "legal binding contract(s)" and mainly controlled by one side, discourages teamwork and reduces efficiency. This approach, which may be used in integration, is not suitable for cooperation and collaboration.

Still one more factor is the allocation of a dedicated budget. Without sufficient funding and resources, it is hard to get a task completed. In an integrative environment, there is one

budget authority. Hence, the decision-making is relatively less complicated. As long as there is a budget available and the priority is set for a task, the task will be funded and relevant resources will be accessible. However, in a cooperative environment or a collaborative environment, there are at least two budget authorities. Each entity may have different budget rules and regulations to follow. Consequently, having the task funded from two sides is not an easy undertaking at all.

These are just some of the factors that ought to be considered in deciding how to structure a partnership venture. In the following discussion, these factors and other relevant factors are analyzed. When all these factors are compiled into a set of features, the differences among various types of partnership methods are easily seen. Below is the list of the factors: the type of trust, the type of organizational structure (org structure), whether the leadership or the command and control (C2) for partnership is established, whether the responsibility is assigned, whether the liability of partnership is made known, the type of relationship endorsed, the type of communication used, whether the checks and balances are employed, whether a dedicated budget is allocated, whether relevant resources are made available for partnership effort, the type of approach taken, whether a common process is utilized, whether a dedicated team is set up, whether a common goal is clearly known by everyone involved, whether a shared strategy is formulated, and whether some dedicated tools are identified and utilized. In the table below, the differences in these factors among these three types of partnership methods are listed.

Table 1. Differences among the three types of partnership methods

Factors	Cooperation	Collaboration	Integration
Trust	May or may not have	May have	Have
Org structure	Horizontal	Horizontal	Hierarchical
Leadership/C2	Not designated	May be designated	Designated
Responsibility	Not assigned	May be assigned	Assigned
Liability	Not known	May be known	Known
Relationship	Very loose	Loose	Tight
Communication	Horizontal	Horizontal	Hierarchical
Checks-and-balances	May have	Have	Not have
Budget & Resources	Not allocated	May be allocated	Allocated
Approach Taken	Bottom-up	Bottom-up	Top-down
Common process	May or may not have	May have	Have
Dedicated team	May or may not have	Have	Have
Common goal	May or may not have	May have	Have
Shared strategy	May or may not have	May have	Have
Dedicated Tools	May or may not have	May have	Have

A FRAMEWORK OF PARTNERSHIP

As shown in Table 1, cooperation, in general, provides a loose and informal working environment. Specifically, the cooperators work in an informal and horizontal management environment, in which they can choose their own ways of performing a task. They do not care too much about leadership and responsibility for a task. Their informal communication is smooth. While cooperating, the bottom-up approach is utilized. They may not have a special and dedicated budget. There is no common process to follow. As they are all task-oriented, they may not have a common long-term goal and shared strategy, and they may not use commonly dedicated tools.

The table above also clearly shows the parameters of collaboration. In general, collaborators still have flexibility in an informal but motivated work environment. Specifically, the collaborators can still work in an informal and horizontal management environment, in which they are motivated to take the lead and take responsibility. As they are in an informal relationship, they may easily communicate with each other. Within this environment, checks and balances are employed; the bottom-up approach is utilized; a special and dedicated budget is approved; and a dedicated team with people from both sides is formed. In addition, the collaborators may have the same common goal and the shared strategy; they may use the same dedicated tools.

Besides, the table reveals the characteristics of integration, which, in general, creates a formal working environment that is better managed with less flexibility offered. Specifically, people work in a formal and hierarchical management environment. They are in a formal relationship. The communication reflects a hierarchical structure. Within this environment, employing an outside organization to conduct checks and balances is usually not an option for various reasons; the top-down approach is utilized; a special and dedicated budget is approved and used; and a dedicated team with dedicated management is formed. Besides, people in a team have the same common goal and the same strategy. They use the same dedicated tools.

It is evident that this analysis, with the help of these relevant factors, can successfully reveal the differences among these three types of partnership methods. After a careful analysis, one may find out that these factors fall into three major categories, i.e., leadership, strategy & implementation, and resources. The relationship among these three categories is shown below:

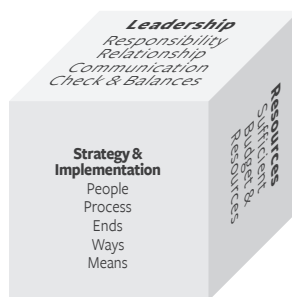


Figure 5. Three categories of factors that determine different types of partnership methods

The parameters of these three categories determine the differences of the partnership methods, which obviously have different levels of requirements for partnership effort. Based on the mission, requirements, needs, and severity level of the environment, an organization can now pick and choose an appropriate partnership method with the help of these three categories of factors. The guidance provided by the proposed framework definitely speeds up the selection process.

The level of severity in an environment also has a say in the selection of an appropriate partnership method. For instance, if the severity level is low, the cooperation method is preferred in most cases. If the severity level is medium, the collaboration method is usually selected. If the severity level is high, the integration method is typically chosen.

For instance, in a national security crisis, an integrated task force needs to be formed and put into action. Within this formal working environment, the hierarchical management is practiced. So is the top-down approach. There is little to no flexibility. With the same goal and strategy and with a dedicated budget, the chance of success for the mission is greatly increased.

This proposed framework can not only distinguish different types of partnership methods with the help of the list of factors but also provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements. In the next section, the advantages of this framework are discussed, and future research is also recommended.

4. DISCUSSION

The proposed framework is able to offer several advantages. First, it clearly differentiates three types of partnership methods. Being aware of the parameters of each method, one can quickly make a decision of which partnership method should be chosen based on one's mission, requirements, needs, and the severity level of the environment. This can serve as a useful decision-making instrument for leaders.

Second, it fully utilizes the effective leadership skills. Building trust, delegating leadership roles and responsibility, encouraging communication, providing a flexible, informal but motivated working environment, adopting the bottom-up approach, and offering financial support are just a few good examples. All these give people in the private sector incentive to actively engage in helping the common public good and national security. They become motivated rather than being forced to share their talents and commit resources. As a result, a strong bond is created between the government and the private sector in handling the challenges in national security. Also, given this framework, the "power over personnel and resources," in Alford and Greve^[18]'s term, can be shared; the state of partnership as power sharing, as Linder^[19] calls it, can be achieved; control and governance, in Bochoven^[20]'s term, can be increasingly shared and collaboration boundaries can thus be broken; and the role of the private sector, as Carrapico and Farrand^[21] argue, can be changed "from objects of regulation to regulation shapers."

Third, it promotes the best practice in strategic thinking. On one hand, it lets partners from both sides figure out a common goal and a shared strategy. It can bring partners with different backgrounds together in tackling the same challenges with their unique talents and perspectives. This joint effort can yield unexpected results in figuring out effective solutions. Naturally, this can successfully address the issue of lacking clear objectives and the issue of “wide gaps between public and private sector expectations,” as discussed by Zhang^[22]. On the other hand, tools like checks and balances can be employed to prevent, detect, and correct errors, issues, and problems while promoting professional environments.

Fourth, it helps to develop leaders who will be efficient and effective in leading partnership efforts in any environment. Specifically, the framework enables leaders to improve three skills essential for leadership, i.e. technical skills, human skills, and conceptual skills. The three-skill approach is the essential component of Katz^[23]'s model in leadership research. It also helps leaders learn how to work with common, diverse, or conflicting goals while “being both participative and authoritative” in a partnership effort, as suggested by Connelly et al.^[24] as well as O’Leary and Vij^[25]. Ultimately, it provides them with an environment in which they can practice “compromises, humbleness, broad-mindedness, ability to work in settings where power is dispersed, and also high conceptual skills (e.g. working with visions and abstractions),” as recommended by Uhr^[26].

There are some areas that need to be addressed. As the framework proposed in this article is at a high level, the inner-workings and details at the low level need to be worked out, especially for collaboration. Besides, this framework has not been tested in real-world environments yet. In addition, metrics have not been developed to measure the effectiveness of this framework.

Hence, future research should be focused on figuring out the inner-workings and details at the low level as well as metrics that can be used to evaluate and measure the effectiveness of the framework. Once done, the framework needs to be tested in various real-world environments to find out its real practical value. Meanwhile, the framework needs to be assessed and its effectiveness needs to be measured and evaluated.

5. CONCLUSIONS

Cyber defense against cyber threats requires the whole-of-society approach, which calls for partnership among the whole society, especially the partnership between the government and the private sector. Partnership can yield a great number of good outcomes for both the common public good and national security. However, it requires leadership, team-building, budget, resources, and strategy. There are different partnership methods for different goals. Without a better understanding of varied requirements for different partnership methods, one may fail to choose the most appropriate partnership method for a specific environment.

To address the issues in the current approach, such as lack of leadership, lack of responsibility, and lack of explicit parameters for partnership effort, a novel framework that incorporates a spectrum of partnership methods is proposed. In the current version, it consists of cooperation, collaboration, and integration. Three major categories of factors—namely leadership, strategy & implementation, and resources—are used to explicitly differentiate the different types of partnership methods. This framework can provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements. Other than these capabilities, this framework is able to fully utilize effective leadership skills, promote the best practice in strategic thinking, and help develop leaders who will be efficient and effective in leading partnership effort in any environment. 🛡️

Author Bio

Professor Jim Q. Chen, Ph.D.

Dr. Jim Q. Chen, Ph.D. is Professor of Cyber Studies in the College of Information and Cyberspace (CIC) at the U.S. National Defense University (NDU). His expertise is in cyber warfare, cyber deterrence, cyber strategy, cybersecurity technology, artificial intelligence, and machine learning. Based on his research, he has authored and published numerous peer-reviewed papers, articles, and book chapters on these topics. Dr. Chen has also been teaching graduate courses on these topics. He is a recognized expert in cyber studies and artificial intelligence.

ACKNOWLEDGEMENT

The author of this article is grateful to Mr. Antonio Rosa and Dr. Corvin J. Connolly at the Cyber Defense Review (CDR), the Army Cyber Institute (ACI) at the U.S. Military Academy (USMA), Dr. Jeffrey D. Smotherman at the U.S. National Defense University (NDU) Press, Mr. Michael Miklaucic at the U.S. National Defense University PRISM Journal, and the blind reviewers for their helpful comments and suggestions for the previous version of this article. Any error in the article is still the responsibility of the author.

NOTES

1. Editor in Chief of Joint Force Quarterly, (2019), An Interview with Paul M. Nakasone. *Joint Force Quarterly* 92 (1), 4-9.
2. B. Obama, (2016), U.S. Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination. Washington DC: The White House.
3. W. Clinton, (1998), A National Security Strategy for a New Century. Washington DC: The White House.
4. G. Bush, (2003), The National Strategy to Secure Cyberspace. Washington DC: The White House.
5. B. Obama, (2011), International Strategy for Cyberspace. Washington DC: The White House.
6. D. Trump, (2018), National Cyber Strategy of the United States of America. Washington DC: The White House.
7. F. Maude, (2011), The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. London: Cabinet Office.
8. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
9. B. Obama, (2013), U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, Washington DC: The White House.
10. N. Blacker, (2017), Winning the cyberspace long game - applying collaboration and education to deepen the U.S. bench, *The Cyber Defense Review* 2 (2), 21-30.
11. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
12. R. Wettenhall, (2003), The rhetoric and reality of public-private partnerships, *Public Organization Review* 3 (1), 77-107.
13. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
14. J. Healy, (2017), Who's in Control: Balance in Cyber's Public-Private Sector Partnerships, *Georgetown Journal of International Affairs* 18 (3), 120-130.
15. S. Osborne, (2002), *Public-Private Partnerships: Theory and Practice in International Perspective*, London: Routledge.
16. M. Manley, (2015) Cyberspace's dynamic duo: forging a cybersecurity public-private partnership, *Journal of Strategic Security* 8 (5), 85-98.
17. K. Eichensehr, (2017), Public-private cybersecurity, *Texas Law Review* 95, 467-538.
18. J. Alford and C. Greve, (2017), Strategy in the public and private sectors: similarities, differences and changes, *Administrative Science* 7 (35), 1-17.
19. S. Linder, (1999), Coming to terms with the public-private partnership: a grammar of multiple meanings, *American Behavioral Scientist* 43 (1), 35-51.
20. L. Bochoven, (2016), Industry and policy: partnerships in disruptive times, *Connections: The Quarterly Journal* 15 (2), 19-29.
21. H. Carrapico and B. Farrand, (2017), Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers, *Crime, Law and Social Change* 67 (3), 245-263.
22. X. Zhang, (2005), Critical success factors for public-private partnerships in infrastructure development, *Journal of Construction Engineering & Management* 131 (1), pp 3-14.
23. R. Katz, (1955), Skills of an efficient administrator, *Harvard Business Review* 33 (1), 33-42.
24. D. Connelly, J. Zhang, and S. Faerman, (2008), The paradoxical nature of collaboration, *Big Ideas in Collaborative Public Management*, edited by L. Bingham and R. O'Leary, Armonk, New York: M.E. Sharpe, 17-35.
25. R. O'Leary and N. Vij, (2012), Collaborative public management: where have we been and where are we going? *The American Review of Public Administration* 42 (5), 507-522.
26. C. Uhr, (2017), Leadership ideals as barriers for efficient collaboration during emergencies and disasters, *Journal of Contingencies and Crisis Management* 25 (4), 301-312.

Civilians 'Defending Forward' in Cyberspace

*Aligning cyber
strategy and
cyber operations*

Dr. Matthew J. Flynn

ABSTRACT

Examining the 'defending forward' concept and the intersection between DoD and the private sector speaks to aligning instruments of national power to set the stage for the consolidation of Internet connectivity and an expansion of that capability. Both outcomes feed a new understanding of what a professional military does in the cyber age to safeguard a civilian interface that is revamping the norms of government across state boundaries. Implementing an effective cyber strategy necessitates recasting the US military's cyber operations to support civilian efforts. A dramatic point of departure from the current emphasis, this change in focus will prevent the US military from leading a non-violent conflict at odds with war in the corporal world. Instead, civilians will be charged with winning the fight in the cognitive arena of cyberspace.

Civilian entities have put themselves in a state of readiness in terms of cyber security that begs the question of exactly what role the US military should play in cyberspace. In several ways, private business is 'defending forward' and waging war in cyberspace, overtly at times. This effort means that the civilian sector seeks to disrupt and halt malicious cyber activity at its source, and degrades such activity before it can reach its intended victims, in parallel with the aim of the Department of Defense's (DoD) new mandate of defending forward.^[1] Detecting and reporting threats from malicious online actors, revealing how those actors frequently work at the behest of nation states, and offering exploits to counter such activity are essential elements of the DoD's active preparedness in cyberspace.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

This positioning also means an attempt to exceed the defense of critical resources and related sectors of the economy to engage in a messaging war that accompanies technical attacks and threats in cyberspace. Yet, the private sector already engages in an online information offensive, and in so doing counters the potential of an inimical US military presence in cyberspace looking to police thoughts exchanged on the Internet. Recognition of the private sector's needed ability to check military largess in this capacity is only slowly coming into focus, but may well constitute the most important measure of the defending forward strategy.

This article calls for the US military to accept the civilian defense of an open Internet that is critical to the success of the future of cyberspace. Leveraging the status quo of "openness" centers attention on the Clausewitzian contest of wills in order to pursue a change in mindset more than a correction in behavior assumed to accompany an act of military force. Defending forward in cyberspace with civilians in the lead can achieve a lasting impact via an act of coercion that seeks a cognitive end, less a physical measure. That intellectual application of war, the most essential measure of a contest of wills, is well-suited to the ether of cyberspace.

In providing a service facilitating a population's access to the Internet and doing so without government oversight, the private sector has delivered the most important function of openness. Whether by balloons, drones, or satellites, these companies provide connectivity to some three billion people and now look to connect the rest of humanity, a further five billion people. This goal may prove overly ambitious, but it means that the number of people online will continue to rise. Even assigning the self-interested motive of gaining market share to those businesses so engaged does little to forestall the reality that with more people online, connectivity remains a powerful reality and so too openness.

A society welcoming openness clashes with authoritarian regimes that recoil before the universal right of users to uncensored information and privacy inherent in a globally connected world. In this democratic purpose lies the intellectual battlefield of cyberspace. Yet, leaders in technology advance openness seemingly oblivious to the ideological implications of what they are advocating. Mark Zuckerberg, CEO of Facebook, proudly issued a call to connect the world when he stood before the United Nations (UN) in September 2015 and identified greater connectivity as "one of the fundamental challenges of our generation." Bringing online access to a further four billion people will empower humanity economically and even socially, he argued. Zuckerberg's UN declaration advanced Facebook's policy from the year before.^[2] In taking this stand, there is no recognition of the cyber ideology embedded in openness that underscores the political ramifications of being online, or the potential for pushback from states threatened by ever broadening Internet access.

The inconsistency of those in the private sector who advance a natural progression towards online interaction, all the while refusing to acknowledge that connectivity invites political plurality, allows government officials to pursue cyber sovereignty. But trying to apply territorial restrictions to cyberspace invites unwarranted military action to curb public expression to

enforce borders in the domain. That effort heightens threats of war that, if acted on, could cripple openness. The risk looms large enough to prompt Microsoft president and chief legal officer Brad Smith to openly appeal for a Digital Geneva Convention in order to prevent cyber conflict that threatens civilian access to a global Internet. In early 2017, he warned an audience at the RSA conference on IT security in San Francisco that the perversion of the medium is at stake and that a cyber war could undo the universal norms of the platform. While governments have a long history of negotiating and observing international rules to restrict the impact of military actions against civilians, Smith argued that business should lead a call on behalf of safeguarding cyberspace.^[3] That a private entity co-opted treaty norms restricting military actions underscores the urgency of business to take the lead in defending openness, thereby, albeit unintentionally, taking the lead in defending forward.

Any brokering of peace in cyberspace will require recognition and, to some extent, legitimization of the ideological struggle in that domain that comes with openness. Despite the absence of international conventions or other agreements to call out this distinction, ideological battles over openness are already underway, with civilians in the lead. The civilian-led fight—no matter how unwittingly—ranges from more or less innocuous websites verbally supporting activist movements to websites offering activists tools for defying online censorship by the outright unblocking of Internet traffic. These services include a VPN offensive targeting specific nations that look to restrict the online communications of their citizens. The progression of a means to promote openness moves from providing a service, to enabling defiance, to direct attack that, when taken together, reflect the capacity of the private sector to defend forward in cyberspace.

Organizations that offer platforms that provide openness as a common good instill hope among online users who might otherwise despair. A number of global citizen networks provide this form of service. For example, the Thai Netizen Network, founded in December 2008, advocates for civil rights and democracy online.^[4] That body upholds the broadest tenets of openness in the face of a strong reactionary movement in Thailand. In February 2019, the Thai government passed a cybersecurity bill creating a government agency to restrict Internet access in the name of countering cyber threats. The National Cybersecurity Committee, answerable to the prime minister, can now use the broad language of the law to ensure the regulating authority of the state to enforce standards and restrictions on Internet access that accord with government concerns that touch every aspect of online use. In short, in a government dominated by a military presence, authoritarianism took a huge step forward in heading off public dissent by enforcing cyber security laws, but global citizen networks, as civilian entities, can circumvent these limits.

Other nations in the Southeast Asian region took similar steps to curb supposed abuses inherent in the cyber medium to make it "safe" for users by thwarting access to information. Vietnam passed a "Cyber Security Law" effective January 1, 2019. In very clear language, the law curtails openness online. One provision of the law, Article 16, prevents "propaganda"

against the state, banning “information contents which incite riots, disrupt security or cause public disorder, which cause embarrassment or are slanderous, or which violate economic management order.”^[5] In Indonesia in January 2018, President Joko Widodo appointed Major General Djoko Setiadi as chief of the country’s new National Cyber Encryption Agency (BSSN), an agency that operates under direct presidential control. This “cyber command” targets fake news, crime, and online extremists. It also sparks fears of eroding civil liberties. By the end of 2018, Indonesia’s legislature started to weigh the merits of a cyber security bill. That effort is pending.^[6]

In many ways, these nations are following the lead of China. That nation’s “Internet Security Law” became effective on June 1, 2017. The government carefully targeted the law to silence online voices that might spur or coordinate civilian activism. Article 12 demands that users “...must not use the internet to engage in activities endangering national...interests; they must not incite subversion of national sovereignty, overturn the socialist system...or disseminate false information to disrupt the economic or social order... .”^[7] This sweeping indictment of Internet functionality also underscores the platform’s capacity for enabling political activism and the regime’s vulnerability to the mere act of connectivity. Openness triggers this counter move from closed regimes, a tension that plays out across Southeast Asia and the Pacific as the region’s power centers employ cyber security measures to target openness as inimical to state interests, challenging the democratic process.

In response to state repression comes a civilian online response. The Asia Internet Coalition seeks “to promote the understanding and resolution of Internet policy issues in the Asia Pacific region.”^[8] Its members include Google, Facebook, Amazon, Twitter, and Apple. This consortium exerts obvious international financial clout. With that standing and, therefore, influence, comes the latent threat of demanding online access for all users, free of oversight, since oversight complicates business practices. Far from a union of state and commercial interests, the coalition stands in defiance of any government seeking to limit user access to maintain control.

Business appears ready to take things even further as the tech industry improves encryption protection to curtail eavesdropping by government on Internet communications. Many companies can scramble information so it can pass data onto an end user without its content being discerned. At the same time, many other companies promise decoding of encrypted communication to forestall potential threats to networks from malware and unwanted intrusion or messaging. In offering a fix, these companies promise relief from increasing cyber threats and offer beleaguered governments a chance to find their footing. Worse, many powerful tech companies have bowed to the demands of overtly authoritarian governments to tailor their interfaces to prevent the user from enjoying unfettered online access. In the case of Facebook, the company has argued that a limited inroad is better than no inroad at all.^[9] This give and take illustrates the clash of values between the cyber self-determination of users and the control of access by self-declared cyber-authorities online. The cyber domain is at once an open space inviting free and unconstrained human interaction but as such it also draws attempts at governmental

control of that very impulse. That duality of cyberspace remains simply too threatening for most societies to leave unpoliced. That tension puts the tech industry at the heart of brokering the means of governance at the expense of government, a tension that has placed defending forward in the hands of civilians.

Parts of the world other than Asia also face similar online challenges. European nations began to test legal measures featuring government oversight of Internet openness to thwart online disinformation. This counter to Russian attempts to influence European elections was a move toward censorship via tighter government controls. Having just endured such meddling in its 2017 presidential election, in July 2018, the French National Assembly drafted two laws to prohibit the manipulation of information online. The proposed changes to the Electoral Code required social media companies to alert users to false information and allowed a judge forty-eight hours to declare the content harmful and to be removed. This mechanism would be enforced three months prior to a national election. Citing the difficulty of making such a determination in a short timeframe, the French Senate rejected the measure at the end of 2018.^[10] The year before, a similar law in Germany survived the two chambers of the legislature. Germany's Network Enforcement Act became effective on October 1, 2017. The so-called "Facebook Act" looked to combat hate speech and fake news posted on social media by demanding social media outlets remove material deemed "unlawful" within 24 hours of notification, or face large fines.^[11] The difficulty of determining what was harmful and therefore unlawful went unchallenged.

In confronting the fear of manipulated information, European nations were striving to preserve their democratic ideals, but felt the same temptation to sacrifice freedom for order and safety as plagued Asia. Fortunately, civilian organizations arose and took on the challenge of documenting online attacks on truth. In 2015, the European Union (EU) created a task force to document examples of pro-Kremlin disinformation carried in the media. The EU vs. Disinfo website publishes a "review" of such abuses, all pursued and substantiated by civilian activists. The webpage offers an indictment of those propagating misinformation, a charge that grows stronger with the passage of time and the growing accumulation of falsehoods.^[12] Ukrainians established "Stop Fake," a fact checking site designed by journalists, students, and IT specialists to rebut fake information about Ukraine and EU states.^[13] This accountability movement modeled a path that avoided censorship via government controls or public vigilantes, advocating as their call to arms that the population become better informed via websites. The Stop Fake model leverages democracy's strongest attributes, its citizens, and moves society away from allowing government agencies to police information and open communication. The EU took this logic a step further when guaranteeing user control of personal data with the General Data Protection Regulation (GDPR) directive of May 2018. By demanding company accountability in the digital sphere on behalf of consumers, the EU struck a delicate balance between government oversight and free enterprise. By looking to empower citizens, a step toward tyranny has been averted.

Russia did not resist that temptation. President Vladimir Putin hoped to cement state online control via laws designed to ensure government authority over all Internet communication. That legislative wall suffers from many cracks, however. For instance, news outlets reported that some 15,000 protesters gathered in Moscow on Sunday, March 17, 2019, after Parliament advanced a digital sovereignty bill creating a government center for monitoring and controlling public communication networks.^[14] The Russia effort to restrict Internet access amounts to censorship in the name of national security much as did Soviet decrees trying to shape culture via government ordinance. Neither effort worked in practice. The same goal to control drove the recent law that merely capped a long-pursued effort to reign in the Internet, allowing Russian government officials to punish individuals with fines or jail time for publishing “unreliable” information online that “disrespects” the state and society. Public statements from Russian officials asserted that the government merely needed to crack down on fake news, much as political figures in western states declare they need to do.^[15] The impracticality of such state supervision means that the cyber frontier stands ready to welcome Russian activists, if not in the name of democracy, then in the name of governance surpassing barriers to achieve a cognitive freedom. The attempt at control primarily expresses the worry of authoritarian leaders in the face of practical limits on curbing public activism and dissent online.

The civilian response enjoys support from a systematic effort among online organizations willing to engage the issue of how best to protect access to information. The veiled threat coming from users sharing networks and making openness real yields to those determined to deliver on that promise. An entire industry of skilled IT professionals supports those calling for connectivity. Access now, for instance, declares its mission as preventing Internet shutdowns. By outing violators and those looking to sabotage the Internet, this organization “fights shutdowns around the world.” This body also publishes a statement of ideals defending openness with the observation that, “The Internet enables all our human rights, and we need our leaders to pledge to #KeepItOn.”^[16] Another example highlights the actions of NGOs. AGORA International, a group of lawyers advocating for human rights, denounced Russia’s efforts to restrict Internet access in a document titled, “Russia. Internet Freedom 2016: On a War Footing.”^[17] While what constitutes a war footing goes conspicuously undefined, the efforts of the Russian government to stymie online access is documented in alarming detail. Putin’s war against sharing information is moved from secret and invisible to shamefully clear.

The escalation from innocuous pronouncements to relatively more aggressive declarations soon gives way to providing tools for direct assaults on those curbing online freedom. The VPN war on closed states continues. China remains a target and a host of companies offer access to the Chinese people without PRC approval, thereby purporting the message of openness. For example, GreatFire.org, an anonymous organization based in China, claims to “monitor and challenge internet censorship in China.”^[18] It offers web applications to do just that, including a browser that delivers uncensored news, electronic access to banned books, and re-published

censored information from WeChat and Weibo, China's most popular social media applications. Tech experts have also turned their attention to Russia. A number of services such as CYBERGHOST connect users to Telegram, the VPN in Russia that evades and defies government control. A website called VPNMENTOR lists the many VPNs that do the same thing in Iran and China as well as Russia i.e. enabling Telegram and making that VPN a means of communication for users seeking a voice in authoritarian states.^[19] Other organizations seek to expand this offensive beyond merely VPN service. LANTERN is a US-government-funded open-source proxy service developed by Brave New Software and initiated in 2013, that looks to "bypass internet censorship and firewalls" to "secure access to an open internet." DEFLECT is a website security service that protects its clients, such as those sponsoring the *Black Lives Matter* website, from distributed denial of service (DDoS) attacks and in that way defends "civil society and human rights groups from digital attack."^[20]

VPN services and related technology receive avid endorsement from the business community. The Open Technology Fund (OTF) provides financial assistance to those engaged in that endeavor. OTF declares its purpose in the familiar language of optimism about humanity's reach for openness. An OTF statement lays out the problem: "The communication of people in more than 60 countries around the world are regularly censored, surveilled, and blocked." To stop these practices, the fund will "support technology-centric solutions." In this way, the organization defies those states that "deny millions of people access to a democratic way of life and positive social change."^[21] Advocating for this fundamental human right joins the ideological struggle over connectivity in cyberspace.

The business alliance continues apace. The Cybersecurity Tech Accord "promotes a safer online world by fostering collaboration among global technology companies... ." That purpose rests on four shared values among all signatories: a strong defense, no offensive actions, capacity building, and collective response. Common purpose will bind the online world together through broad use of these best practices featuring collaboration that hardens defenses to frustrate exploitation of vulnerabilities, a step fundamental to improving the reliability of products and services. Still, the concept of better security via shared commitments to cooperation across the "wider global technology ecosystem" is a familiar notion to those accustomed to the language of conflict deterrence. Emphasizing defense, discouraging attack, and building alliances mirrors the logic of diplomatic and military agreements among states. However, in the context of Internet access, this deterrence effort binds over 100 companies "committed to protecting cyberspace," including familiar powerhouses in cyber technology such as Microsoft, Intuit, CISCO, and Facebook.^[22]

That language paralleling a military footing is intentional, as Microsoft President Brad Smith made explicit when he spoke at the RSA Web Summit in Lisbon, Portugal, in November 2018. In his address, Smith went to great lengths to demand that the technology industry assert itself in the ongoing cyber war. He said, "Like it or not...the reality is nonetheless inescapable. We

have become the battlefield.”^[23] That declaration accepted defending forward as the de facto truth, a mandate staring the business community in the face and requiring a response. That response could only take one form: the tech community waging the cyber war by recognizing its ability to compel states to resolve their differences by means short of military action.

The business community surpassing the US military in terms of defending forward in cyberspace points to the latter’s slow recognition of the strategic advantage stemming from openness—an ideological offensive resting on technological development that both continues the quest for universal online access and arrests a military push to secure cyberspace on behalf of government that threatens that very pursuit. Greater clarity means the conversation on cyber policy should turn away from the reflexive impulse to ‘strike back’ to support preserving openness. Since advancing an open, secure, stable, accessible and peaceful cyberspace is US cyber policy, and it largely goes unrecognized, something must be done to make clear that this stand is sound policy, and one predicated on a whole of government response.^[24] This need means maintaining a preponderance of US military power with a global reach to limit violent conflicts that threaten to escalate. It also means that after delivering this deterrence, the US military has a limited role to play in cyberspace. Here, defending openness requires efforts to blunt the call for cyber sovereignty and instead broker international agreements to protect a global commons, ensure government allegiance with private industry to shore-up the credibility of social media, and foster government support of the private sector advancing openness as a universal human right in cyberspace. That ideological campaign already stands at the heart of US cyber policy. In short, little has to change other than that US cyber policy must be recognized and accepted as sound policy among its critics.

In failing to grasp this pivot, the United States cedes the defense of Internet openness to the international community. France hosted a “Paris Call” for building “trust and security in cyberspace” on November 12, 2018. While the United States failed to attend, sixty-five states, 138 civil society organizations, and 344 entities of the private sector did attend, reaffirming the decree to uphold “an open, secure, stable, accessible and peaceful cyberspace.”^[25] The US government’s absence accentuated the new militarism unfolding in cyberspace thanks to the effort of the private sector, an effort demanding cognitive struggle as a norm and something unfolding without violence as a means of settlement. This mandate informs a US cyber policy that now rests in the hands of the US military charged with striking back in cyberspace via defending forward. That strategy undermines the effectiveness of the civilian mission of defending forward by imposing one’s will on an adversary with the ideological war for openness. Instead, in the US model, nonviolent actions are military acts by military actors. This incongruity represents a clear point of departure from other states organizing to wage the cyber war as a mission of peace-minded, private organizations looking to hold states in check in cyberspace.

The Paris meeting built upon some very specific and pointed antecedents. Previous, tentative calls for a cyber treaty had unfolded to manage the developing crisis in cyberspace. The efforts foundered, unsurprisingly, overcome by the impossibility of appropriating the existing norms and constructs of international relations. Borders, alliances, monitoring verifiable arms and, most significantly, recognizing a threat to one's vitality, all faced obfuscation in cyberspace when government became the agent of control. Governance proves the larger and more meaningful arbiter of international norms, no matter its apparent unwieldiness. Civilians have grasped this new reality and the need to get beyond an embrace of war terminology in pursuit of nation-state security in the new age. The call for online access as an endorsement of freedom of expression and openness means recapturing the inspirational appeal of those seeking to excel at technological prowess. In that light, defending forward becomes the foremost quest in cyberspace thanks to a civilian body embracing its call to champion conflict that unfolds in that cognitive sphere without the traditional trappings of physical conflict as war which has accumulated centuries of authority. The US military would do well to ensure its cyber operations support this larger strategic focus.♥

Author Bio

Dr. Matthew J. Flynn

Matthew J. Flynn, PhD., is Professor of War Studies at Marine Corps University, Quantico VA. He specializes in the evolution of warfare and has written on topics such as preemptive war, revolutionary war, borders and frontiers, and militarization in the cyber domain.

NOTES

1. For the formal articulation of defending forward as reaching beyond DOD networks and countering adversaries in the era of persistent engagement, see “Summary: Department of Defense Cyber Strategy,” DOD, 2018: 1, 4; and “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” April 2018: 4, 6.
2. “Facebook CEO Mark Zuckerberg at the UN,” September 26, 2015, <http://www.un.org/pga/70/2015/09/26/facebook-ceo-mark-zuckerberg-at-the-un/>, accessed September 27, 2015. See Mark Zuckerberg announcing that Internet.org will seek to make “basic internet services available to every person in the world.” Mark Zuckerberg, Facebook, March 27, 2014, <https://www.facebook.com/zuck/posts/10101322049893211>, accessed April 26, 2015. See Facebook’s goal of connecting “the next 5 billion people” in, “Is Connectivity a Human Right?” an undated 10-page document at the following address: <https://www.facebook.com/isconnectivityahumanright>, accessed April 26, 2015.
3. Brad Smith, RSA Conference, “The Need for a Digital Geneva Convention,” February 14, 2017, San Francisco, California: <https://www.youtube.com/watch?v=C-YvpujO6pQ>, accessed May 8, 2019. And, “The Need for a Digital Geneva Convention,” Brad Smith, Microsoft, Blog Post, <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001f0wujpo0tdrhytq2edlwmgn9i>, accessed May 15, 2019. See also Microsoft Policy Paper, “A Digital Convention to Protect Cyberspace,” no date.
4. Thai Netizen Network, <https://thainetizen.org/about>, accessed July 8, 2019.
5. “Law 24 on Cybersecurity, dated June 12, 2018,” Chapter 3, Prevention of and Dealing with an Infringement of Cybersecurity, Article 16, page 11, from Vietnam Laws Online Database, Allens International Law Firm, www.vietnamlaws.com, accessed July 8, 2019.
6. “Indonesia’s New Cyber Agency Looks to Recruit Staff of Hundreds,” Kanupriya Kapoor, *Reuters*, January 5, 2018. See reference to, “Bill on Security and Security of Cyber,” National Legislation Program, Board of People’s Representatives of the Republic of Indonesia, www.dpr.go.id/prolegnas/index/id/223#, accessed July 8, 2019.
7. Article 12, “Cybersecurity Law of the People’s Republic of China (Second Draft),” translation by the American Chamber of Commerce - China, no date.
8. Asia Internet Coalition, “About,” <https://aicasia.org/about/>, accessed July 8, 2019.
9. Mark Zuckerberg, Facebook Post on March 16, 2015, <https://www.facebook.com/zuck/posts/10101974380267911>, accessed March 17, 2015.
10. “Senate Rejects ‘Fake News Ban’ Bills,” September 24, 2018, Global Legal Monitor, The Law Library of Congress, www.loc.gov/law/foreign-news/article/france-senate-rejects-fake-news-ban-bills/, accessed July 9, 2019.
11. “Social Media Platforms to be Held Accountable for Hosted Content under ‘Facebook act,’” July 11, 2017, Global Legal Monitor, The Law Library of Congress, www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountalbe-for-hosted-content-under-facebook-act/, accessed July 9, 2019.
12. EU vs Disinfo, “About,” <https://euvsdisinfo.eu/about>, accessed July 9, 2019.
13. Stop Fake, “About,” <https://stopfake.org/en/about-us/>, accessed July 9, 2019.
14. “Russia Internet Freedom: Thousands Protest Against Cyber-security Bill,” *BBC*, March 10, 2019.
15. Shannon Van Sant, “Russia Criminalizes the Spread of Online News Which ‘Disrespects’ the Government,” NPR, March 18, 2019.
16. Accessnow, #KeepItOn, What is an Internet Shutdown, <https://www.accessnow.org/keepiton/>, accessed July 12, 2019.
17. *Russia. Internet Freedom 2016: On a War Footing*, Report, AGORA, 2016.
18. GreatFire.org, English Version, <https://en.greatfire.org>, accessed July 12, 2019.
19. VPNMentor, 5 Best VPNs for Telegram in Russia in 2019 [only those work], <https://www.vpnmentor.com/blog/unblock-telegram-russia-with-best-vpns/>, for Iran, 5 Best VPNs for Iran, <https://www.vpnmentor.com/blog/best-vpns-for-iran/>, for China, 9 Best (Still Working in July 2019) VPNs for China,” <https://www.vpnmentor.com/blog/5-best-vpns-for-china-verified-list/>, accessed July 12, 2019.
20. Lantern, https://getlantern.org/en_US/index.html, accessed July 12, 2019; Deflect, Protecting Online Voices, <https://deflect.ca/#our-principles>, accessed July 12, 2019.
21. Open Technology Fund, About, <https://www.opentech.fund/about>, accessed July 11, 2019.
22. Cybersecurity Tech Accord, About: Mission Statement/Values/Signatories, <https://cybertechaccord.org/about/>, accessed July 11, 2019.

NOTES

23. “Digital Peace in the Age of Cyber Threats,” Presentation, Brad Smith, RSA WEB Summit, 2018, Lisbon, Portugal: video 21:30’-21:41’, <https://www.youtube.com/watch?v=d-k5U2Bd3PQ>, accessed July 11, 2019.
24. A US cyber policy that demands the Internet remains open, interoperable, secure, and reliable has been remarkably consistent. See *National Cyber Strategy of the United States of America*, White House, September 2018, 24; Summary, *Department of Defense Cyber Strategy*, DOD, 2018, 1, 7; *Cybersecurity Strategy*, US Department of Homeland Security, May 15, 2018, 4; President Trump, “Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” The White House, Office of the Press Secretary, May 11, 2017, Sec. 3 (a); *International Cyberspace Policy Strategy*, Department of State, March 2016, 2; *Cyber Strategy*, DOD, April 2015, 1; *Strategy for Operating in Cyberspace*, DOD, July 2011, 2; and *International Strategy for Cyberspace*, White House, May 2011, 3, 21.
25. Proclamation, *Paris Call: for Trust and Security in Cyberspace*, November 12, 2018: 1; and see list of signatories.

Norms and Normalization

Dr. Martin C. Libicki

The search for norms has proven to be one of the most frustrating elements of cyberspace operations. Informed consensus holds that there *should* be norms of international behavior to tame the Wild West of cyberspace. Yet, if norms are defined to exist when a country refrains from operations otherwise in its interest^[1] (taking domestic and international politics into account) they do not exist. That is, there are zero such norms that enjoy adherence that matters.

In light of such disappointments, this paper mulls a different approach to thinking about norms. Rather than focusing on what responsible governments should *not* do, it looks at what they actually do as a guide to what activities in cyberspace have effectively been normalized (that is, within *de facto* norms)—and may remain normalized until the rewards from such activities no longer merit the effort.

This argument has three parts. The first part discusses the lack of progress towards norms. The second defines normalization and examines the extent to which the behaviors of specific countries establish what has, in effect, been normalized. The third part focusses on one particular activity—implanting malware into the weapons systems of potential adversaries—as a candidate for normalization.

FROM NORMS

Norms can be understood as rules for behaving that forbid or encourage^[2] certain activity. As with information technology standards^[3] anyone can propose a norm, but to be a successful norm requires that some critical mass of countries adhere to them.

Proposed norms for cyberspace have come from many sources. Three include an extension of the Laws of Armed Conflict (LOAC) from the physical world to cyberspace; negotiations among multiple states; and bilateral agreements, notably the Xi-Obama agreement of September 2015.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

The proposition that LOAC applies in the virtual world as it does in the physical world would seem to be self-evident. Strictures on violations of sovereignty, the use of disproportionate force, gratuitous attacks, perfidy, the violation of neutrality, and so on rest on the belief in fundamental human rights and are therefore medium-agnostic. The Tallinn Manual^[4] epitomizes the LOAC approach. Its technical quality is undeniable. Unfortunately, its scope is quite limited. International humanitarian law (of which LOAC is a component) aimed to modulate death, injury, and destruction from war. Cyberattacks, by contrast, have yet to hurt anyone directly, and very rarely break things in the physical sense. Their toll is measured in time and money, both of which fall outside the scope of LOAC. Granted, the second version of the Tallinn Manual^[5] discusses countermeasures: what one state can do to make another state stop behaviors that levy time and money costs. But a broad right to self-defense allows certain behaviors; it does not forbid unwanted behavior. As for cyberespionage, which is far more common, the Tallinn Manual is silent. Conventional espionage does not fall under LOAC. Thus, ditto for cyberspace espionage—even though the distinction between conventional espionage and armed attack is far clearer than between cyber espionage and cyberattack.

Attempts to craft norms specific for cyberspace have not fared much better. The most official such endeavor is the U.N. Group of Government Experts (GGE). The high-water mark was the 2013 agreement among participating countries (notably the United States, Russia, and China) that LOAC covered cyberspace. But no sooner had Russia's and China's diplomats returned home than both governments concluded that even so simple an agreement was not really what they had in mind. Subsequent GGE sessions fared worse. Although the process revived^[6] in 2019, expectations should be tempered. The closest to a formal norm for cyberspace—in the sense that it is a formal treaty that has been implemented in national law—comes from the Convention on Cybercrime of the Council of Europe (aka the Budapest Convention). It binds members to mutual assistance for cybercrimes. It works well within the group of signatories (e.g., by facilitating the arrests of cyber-criminals), but Russia and China are prominent among the non-signatories, and Russia, in particular, has shielded cyber-criminals from prosecution.^[7] And the Convention imposes no restrictions on what *states* can do in cyberspace. Other initiatives to establish norms include those by Microsoft^[8] and the Paris^[9] declaration. Nice words by states and institutions that never had a desire or willingness to carry out problematic operations in cyberspace are no substitute for actual restraint shown by states that could and often do carry out such operations.

The closest workable norms in cyberspace arose from the personal agreement between President's Xi of China and Obama of the United States (US) to cease cyberespionage against commercial firms for commercial purposes (but bypassed activities such as hacking commercial firms to find exploitable flaws in their products or looking for records of terrorist activity). This agreement was extended globally in a subsequent G20 agreement^[10]. For the first time, a major country had agreed to stop doing something that clearly benefitted it. Alas, while the agreement initially reduced China's cyber-espionage, Chinese cyberespionage levels^[11] apparently

reverted to form in early 2017. The primary difference between then and now is that operators are more discreet in their techniques and target selection.

Two problems bedevil effective norms-making in cyberspace. One would be difficulties in attribution; they allow governments to advocate for restrictions they violate in the belief that can plausibly deny. Granted, rarely does a major cyberattack takes place without one or more cybersecurity companies (and increasingly, governments) assigning blame. Their assessments are usually credible. But the process by which cyberattacks are attributed is opaque and often bereft of details. Governments are particularly reluctant to explain their rationale for their judgments, particularly when they have used sensitive sources and methods to draw conclusions. As a result, those inclined to be skeptical can maintain their doubts. Countries can and do blandly assert that accusations against them arise from animus, not evidence. In fairness, once cases get to court, the evidence is presented and prosecutions often result. Since 2014, the US has been energetic in issuing indictments^[12] against state-hired or at least state-supported actors, suggesting it has similar evidence, but none so indicted have appeared in court.^[13] Increasingly, it seems, your friends will believe your facts and your foes will not. This is not an environment in which good behavior results from fear of credible accusations.

A more significant problem may be that the desire for norms is asymmetric. They are seen as signifiers imposed on misbehaving countries by those who see themselves virtuous. Take the Xi-Obama agreement. China forewent operations that profited them; the US forewent operations that it had no interest in—while giving itself a pass on those types of cyber-espionage against commercial that *did* interest them. There was no comparable behavior from the US that China both wanted to modulate and had a reasonable prospect of so doing in return. No US administration, for instance, could credibly promise to squelch the free speech of dissidents. As a rule, countries agree to asymmetric deals only under coercion. In the Obama era, the threat was sanctions. The Trump Administration, however, signaled that the Chinese were engaged in a large variety of “unfair” trade practices, not just intellectual property theft. Sanctions would, therefore, be coming irrespective of China’s conformance with the Xi-Obama deal. So, why keep its terms? The broader rule applies: norms established in state-to-state negotiations require proponents to give up something as well as receive if such norms are to persist.

From the US (or broadly Western) perspective, matters are unlikely to improve. Relations with Russia turned sour in 2014 (as a result of Crimea). Relations with China did likewise in 2017 (as a result of trade disputes). Disunity in the West has made it harder to reach internal agreement on norms, much less apply unified coercive pressure. It does no good to plead that civilized Western states have advocated and adopted a set of norms-like practices. For the most part, they are not each other’s targets in cyberspace. But the West, in general, does compete with countries such as Russia or China—and to recognize as norms those activities which the West has or would like to abjure is akin to asking for unilateral disarmament hence, not viable.

TO IMPLICIT NORMALIZATION

Consider now a different approach, concentrating on normalization rather than norms. Norms say what states should not do. Normalization says that certain activities are regarded as part of the given environment and likely to stay that way, either because they are deemed legitimate state behavior or because there is no reasonable prospect that they will end. An example of normalized behavior was the Soviet practice of parking trawlers near U.S. naval exercises in open waters (largely to facilitate eavesdropping). The US initially objected to this practice, but when the Soviets proved adamant that their behavior was permitted and not harmful, the US grudgingly accepted this as a normalized state of affairs^[14] Indeed, the impetus for objecting to this or that behavior is often that if it remains undisputed, it will become normalized. British Foreign Secretary Jeremy Hunt's praise of EU cyber sanctions was based on the hope that "We can now impose tough sanctions on those responsible for malicious cyber-attacks. [Otherwise] trying to interfere in other countries' democratic processes is becoming normalized."^[15]

Explicit normalization also helps make the case for norms. As Max Smeets has observed^[16] of the US: there are many practices that raise objections, but few, if any, that are deemed acceptable and will not be challenged. Normalization of some practices makes norms against other practices seem reasonable rather than as a list of generalized complaints. It distinguishes between the permissible and the impermissible.

Putatively, norms and normalization should be like a mold and a casting: the existence of one implies the other because everything is either allowed or it is not. Unfortunately, it is nearly impossible to create a definitive list of cyber operations that can be so evaluated. Surprises—not only what states *would* do but what states *could* do—keep coming. In 2015, when members of the Defense Science Board—a savvy group—tried to enumerate what behavior would cross a US red line, not one of them suggested something like the 2016 DNC hack. But normalization would at least suggest what buckets various operations could fall into.

One example of normalized behavior is that countries are allowed to carry out cyberespionage in support of national security decision-making (much as conventional espionage is considered normalized state behavior). Roughly speaking, an activity is normalized when carried out by at least one capable and serious country—especially if that country does not deny such activity (admitting to such activity is a less realistic prospect) or make excuses about it. This hardly means that other countries accommodate such practices. In many cases, they will object. But if such objections fall on deaf ears and more forceful responses elicit only countervailing pressure by the accused state, then at some point others will concede that such practices are here to stay, and maybe they, themselves, should adopt them. Thus, even if the point is to establish behavior for the other side to negotiate away, for example, another state may adopt a practice that the first state would rather not see. Others also do so. The initiating state may then conclude it would be better off in a world in which such practices were foresworn.

So, *which* country's activities can credibly establish the norms for the rest of the world?

Start with two that would not. North Korea has carried out severely disruptive cyberattacks against targets in South Korea and the Sony Corporation. Its hackers have robbed banks, most notably the central bank of Bangladesh, as well as several digital currency exchanges.^[17] To set North Korea as the standard for normalization essentially normalizes bank robbery. Similarly, Iranian hackers have trashed computers (notably those of Saudi Aramco and Las Vegas Sands Corporation); worse, they have been implicated in tampering with safety systems in industrial facilities. Again, to set Iran as the standard would normalize highly dangerous practices. That North Korea and Iran have essentially put themselves on a war footing (*vis-à-vis* South Korea and Saudi Arabia, respectively) may excuse them. Yet, it hardly normalizes behavior for countries that are not on a war footing.^[18]

Russia presents a problem because it is too big (and too adept in the arts of cyberspace) to be dismissed as a basis for normalization. But Russia's behavior, at least since late 2013, has crossed limits (i.e., taking territory from a neighboring country) that had been adhered to by the Soviet Union once World War II was over. As for cyberspace operations, Russian hackers have interfered in the politics of the US, the United Kingdom, and several other countries. Russian hackers are believed by the U.S. Intelligence Community (IC) to have implanted malware in the electrical grid of the US^[19] and Europe. Russian hackers have corrupted the software and knocked offline the power grid of a state in peacetime. Thus, using Russia as the standard for normalization would require accepting that such activities can be expected from responsible countries. This is broadly unacceptable, not least to the US.

One problem with normalization is apparent in the above: these are all activities that have been attributed to Russia but never acknowledged.^[20] This could present difficulties if Western countries did the same to others, notably Russia, and excused their activities by arguing that Russia's behavior had *de facto* normalized such operations—only to be met by denials that Russia had done what it was accused of. But if Russia *were* to object to cyberspace operations against it, carrying the objection puts the burden of proof on its own shoulders. Arguing that China did it would not dent the West's view that such activities were normalized, it would only shift the blame.

China presents a better case that its behavior can set the standard for what can be considered normalized. Its economy is putatively the world's largest, its population undoubtedly so, and it is increasingly adept at cyberspace operations. In contrast to North Korea, Iran, and Russia, all of whom are trying to upset the world order, China is content with the structure if not necessarily the leadership of the world order. Although China has carried out a great deal of cyberespionage, its *known external* cyberattack activity has been limited to DDOS attacks on dissidents (and dissident-used Web sites such as GitHub). But to accept Chinese behavior as normalized means accepting cyberespionage for commercial purposes, something that China has formally foresworn. And it is difficult to believe that the many BGP (border gateway proto-

col) attacks^[21] ascribed to China have all been accidents—although, if deliberate, their purpose has been for cyberespionage which itself is largely normalized. Nevertheless, would the West be comfortable if China’s behavior *were* the rules of the road?

Before getting to the putative gold standard for cyberspace normalization, it would help to go over the limits of normalization. Normalization does not mean that every country does as much as they are capable of (even if that is a serious constraint on mischief in cyberspace). Countries can abjure operations for political and strategic purposes. Some operations would sit poorly with their polities. Also, many who have advocated against certain practices would be taking risks if they conceded that their words avail naught and do what they have condemned – without at least a nod to their changing standards. Furthermore, just because Russia and China behave in cyberspace in ways that violate what the West would like to see as norms does not mean that they do not operate under their own restraints, perhaps in the hopes that the West would someday follow suit. That said, it is unclear what they refuse to do because it is wrong *vis-à-vis* because it might backfire.

That brings us to the US. Its size, sophistication, and alliance structure all suggest it alone normalizes behavior in cyberspace. Furthermore, the US has, among the powers, been most vociferous in advocating for norms of responsible state behavior in cyberspace, which means that if the US does something, it is unlikely that the US would advocate for its not being done. Finally, although the US does not own up to everything it is accused of, outright false denials are quite rare, particularly in the post-Snowden era.^[22] To wit, whether it wants to or not, US behavior has become the gold standard.^[23]

What might be considered now-normalized behavior because the United States has already done it?

First, the US has, in all likelihood, carried out cyberattacks designed to impede the production of nuclear weapons and their delivery systems. Stuxnet is an example of the first: it was used against Iran, and maybe against North Korea (albeit with no known effect^[24]). Reportedly, the US tried to interfere with North Korea’s production of reliable liquid-fueled intermediate-range missiles.^[25] So, is breaking other people’s weapons behavior that merits normalization? Or are nuclear weapons, in their destructiveness and appeal to rogue regimes, special enough to belong in their own category? Perhaps using cyberspace operations to break the nuclear weapons systems of proliferators can be considered normalized behavior – without necessarily extending the practice to *accepted* nuclear powers^[26] (e.g., China) or other frightening weapons (e.g., hypersonic missiles).

Second, although cyberespionage against individuals is as acceptable state practice as is espionage against them, the US reportedly has surveilled a large body of communications in order to select the handful that represents people of interest.^[27] In a sense, this echoes how it works with traditional radio-frequency signals intelligence – as well as with Defense Advanced Research Projects Agency’s (DARPA) proposed Terrorist Information Awareness. Five to ten

years ago, the Chinese might have objected to such normalization, but their theft of U.S. Office of Personnel Management (OPM) data to (reportedly) find US espionage agents and help recruit their own, coupled with breaches of airline companies (e.g., United and American), health insurers (Primera, and Anthem), hotels (Marriott), and contractors who work personnel clearance (USIS) suggests that they view harvesting hay in pursuit of needles as normalized state behavior.

Third, recent claims of USCYBERCOM activity could normalize new categories of cyberspace operations. One is persistent engagement. Although the specific operation claimed in the press—a DDOS attack to stymie Russia’s Internet Research Agency^[28]—was small potatoes, it is unlikely to be the only such engagement. Accordingly, one must presume that cyber operations meant to interfere with cyber operators on the other side is fair game (even if many of these cyber operators are carrying out cyberespionage, which is a normalized activity). The modest risks of escalation, and the nature of cyberwarrior-on-cyberwarrior combat, aside, this development does not seem to be particularly problematic. The targets have little cause to complain.

Fourth, in early June 2019, the *New York Times*^[29] reported (apparently without pushback from DoD) that USCYBERCOM was stepping up its efforts to insert malware into the Russian grid. This would supposedly deter Russia’s activating the malware suspected to lurk in the US grid.^[30] If true, it signals that the US regards implants in electric grids as already having been normalized by Russian behavior—and that the Administration had too little confidence that the Russians could be persuaded to withdraw their implants or abjure from implanting more malware (although, as with nuclear weapons, the practice of implanting malware can, in theory, be de-normalized by subsequent treaty). Perhaps needless to add, once malware is implanted nothing prevents its use in an opening salvo or being brandished as a deterrent against other unwanted behavior. Of note is that, as a GGE member, the US had agreed that the peacetime use of cyberattacks against critical infrastructure is out of bounds; thus, either such agreement is void, or the presumption now is that Russian cyberattacks against the electric grid are *de facto* acts of war. Again, if press reports of *Nitro Zeus* are correct,^[31] the US had pre-wired Iran’s electric grid *before* reports surfaced that Iran had done the same to the US grid.^[32]

Fifth, in the days after a U.S. Global Hawk was shot down by Iranian batteries, the US purportedly^[33] carried out cyberattacks. Using cyberattacks as a tit-for-tat would appear to be itself unexceptional and does not normalize cyberattacks except against something that looks close to armed conflict. But, if it takes weeks and more likely months to prepare such an attack,^[34] then these implants *preceded* the Iranian attack. Therefore, the US has signaled its right to lay in attacks against military systems of potential adversaries in peacetime. Was this deliberate? It may have resulted from the calculation that the US has more to gain than lose from opening that door. If implants are limited to military systems, rather than extended to dual-use systems, the risk to civilians is limited. Doing so potentially substitutes nonlethal for lethal means of combat. It may have reflected a perception that potential adversaries of the US are unbound

by norms, and thus, why not prepare the cyberspace battlefield if the alternative is to accept a military disadvantage? Or, as per human nature, actions come first and wondering if such actions changed the rules of the game come later.

AND EXPLICIT NORMALIZATION

Now, go one step further. Perhaps the US should explicitly declare that preparing the battlefield through injected implants into (or using comparable means such as credentials hijacking or placing physical devices near to) potentially hostile defense systems is a legitimate state activity. In that sense, such peacetime activity is no less legitimate than is preparing the conventional battlefield through remote surveillance.

Note that announcing that implants are legitimate state activity and inserting implants are two different actions. One can be done without the other. The first essentially says to potential adversaries that the US could be in your military systems in ways that make them malfunction, create safety hazards associated with combat use (creating hazards for peacetime exercise use is a hostile activity), or, at very least, creating telemetry data when they are used (the better to target them with precision weapons). Others may dismiss these claims: Russia^[35] and Iran^[36] both deprecated reported claims to have interfered with their systems. But behind such public sang-froid must lie some degree of concern on the target's part, which at very least will complicate its war planning. Indeed, while military systems fail statistically in combat, the prospect that every weapon of a particular class may fail in a very public matter at the outset of aggression cannot help but temper the confidence that aggressors must feel before they start to war. The prospect of embarrassment may be more daunting than the prospect of defeat. Conversely, such an advantage may be temporary given the contest between measure and countermeasure. In practice, as well, the credibility of an assertion that the US is in the systems of others may require demonstration from time to time. And while the failure to complete an implant may go unnoticed, the failure to exercise an implant in circumstances where others expect it (i.e., when the US has an interest in seeing systems fail then and there) may erode credibility.

The value of such an announcement may also lie in what happens when an implant is discovered in someone else's military system. Under current circumstances, the victims could easily conclude that the implant itself means that combat is coming, and probably soon—ignoring that implantation may have preceded discovery by months and years. Such conclusions may give rise to thoughts of pre-emption.^[37] However, if the US has explicitly indicated that it would, where possible, insert implants in potential adversary systems as day-to-day practice, the discovery of an implant should be less likely to point to imminent conflict. Furthermore, while discovery may indicate that inserting implants is not risk-free, it could also signify that the US talk about implants are not mere words.

The last argument returns us to the problem of norms. As argued above, one reason that the Xi-Obama agreement on cyberespionage is ailing is that it was not a trade in which both parties gained but one made under a one-sided threat and only as good as the threat lasted.

To the extent that other countries fear the US loading implants into military systems works in that they may be amenable to norms in which they give up something they want to do if the US does likewise. They would be inhibited from backsliding by the fear that the US would return to practices they, themselves, disliked.^[38] Perhaps needless to add, attribution issues will face both sides in such a trade. Furthermore, if US cyberwarriors see serious advantage in implantation, they will be reluctant to trade it away (especially for norms without military implication: e.g., against vote-tampering). It would not be the first time that organizations fell in love with their bargaining chips.

A tricky issue may also arise if other countries believe that US cyberspace activities extend to their far more consequential nuclear systems. One need not imply the other. Normalizing implants in conventional military systems is far different from normalizing them in nuclear systems in general or nuclear command-and-control systems in particular. Countries nervous about the viability of their nuclear deterrent can react in ways that make nuclear war—notably inadvertent or accidental nuclear war—more likely. But would a US statement that it would differentiate between conventional and nuclear systems assuage them? In some countries, the two types of systems are entangled.^[39] But even where they are not, simply introducing the prospect of implants may spark fears that could override distinctions that are later offered.

Would declaring an open season for implants on conventional military systems work to the US advantage? Although U.S. cyber operators are second to none, the U.S. military has also embraced digitization and networking far more than others have. Nevertheless, an explicit declaration may remove constraints on USCYBERCOM while having little effect on adversaries who are unbothered by US views on norms. And, such a declaration may not be so far from current practice even among U.S. allies. Florian Kling, who leads a German military watchdog group, holds

that international law allows for preemptive attacks in self-defense if a military strike is imminent, but not preventive attacks; cybersecurity operations lie somewhere in between. ‘We would have to identify gaps in their security and implant a Trojan or virus so that the next time they attack, we can shut down their system ... and therein lies the problem: Is that a preemptive strike, if the opponent hasn’t yet attacked or initiated any actions?’^[40]

There are other sources of caution. With such a declaration, the US loses the ability to hold other countries to account when they infiltrate US systems. Even if the US comes out ahead by opening the arena, U.S. allies—many with far fewer offensive cyberspace capabilities—may lose more than they gain if defense systems become fair game for implants. Would purchasers of US defense products conclude that the normalization of implants in an adversary extends to legitimizing kill-switches in such products (that could be activated in case of misuse or a change in government orientation)? And, finally, there is no guarantee that others will strictly adhere to the same definition of what is normalized. Can the US declare that defense systems are in-bounds for implants but that dual-use infrastructures (e.g., electricity, telecommunications)

are not—only to find that other countries conclude that implants on the latter are normalized by the same logic? Would such normalization suggest that implants in police and/or surveillance systems of other countries are also legitimate extensions of allowing implants into their military systems? If the US normalizes implants but does not normalize their activation except in times of war, would other countries adhere to the same notions of what constitutes war that the US does?

That noted, the admonition not to move thoughtlessly is not the same as the admonition not to move.

CONCLUSIONS

Norms are ideals. Normalization concedes that states do not run on ideals. In theory (and some practice), the West has been promoting ideals to foster a world in which the rule of law rather than the Melian dialogue is a guide to international behavior. But behind these ideals have been countries whose strength—military, but also economic (see sanctions)—helps ensure that these ideals are put into practice. There is no *ipso facto* reason why cyberspace should not be subject to the rule of law, even—perhaps especially—as they affect responsible state behavior. But realistically, after a quarter-century of interest and at least ten years of real work, progress has been disappointing. 2015 appears to have been the high-water mark for the ability of norms to curb unwanted state behavior.

Normalization is the recognition that states will continue to do things in cyberspace, not necessarily to the advantage of other states. But by concentrating not on what is forbidden but by what is permitted through common practice, it is possible to reason by exception to see what the feasible space of norms may be. It grounds the search for norms in *realpolitik* that correctly reflects the ambiguities of activity in cyberspace, and the license it gives actors. Explicit normalization may play a role in this process. In the case presented above, a declaration that military systems may not be considered safe from implants provides many advantages and may spur other countries into taking norms (and concomitant attribution challenges seriously).♥

Author Bio

Dr. Martin C. Libicki

Martin Libicki (Ph.D., U.C. Berkeley 1978) is the MaryEllen and Richard Keyser Chair of Cybersecurity at the U.S. Naval Academy where he teaches cyberwar strategy and cyberspace economics. Prior employment includes having been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. He wrote three commercially published books: *Cyberspace in Peace and War* (2016, second edition forthcoming), *Conquest in Cyberspace: National Security and Information Warfare* (2007), and *Information Technology Standards* (1994). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, *Cyberdeterrence and Cyberwar*, *How Insurgencies End* (with Ben Connable), and *How Terrorist Groups End* (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

NOTES

1. In theory, a state could believe that operation X was to its advantage if its foes did likewise – but not to its advantage if its foes also abjured. So, *other countries'* restraint would not change the underlying fact that the state was optimizing without regard to norms. Plausible examples of this in cyberspace are not easy to find, especially because it is often unclear what one's foes are, in fact, doing in cyberspace.
2. One example of a proposed rule to encourage good behavior is Duncan Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal*, Volume 52, Number 2, Summer 2011, 374-432.
3. On standards, see, for instance, Martin Libicki, *Information Technology Standards: Quest for the Common Byte*, Digital Press, 1995.
4. For the first version, see the 'Tallinn Manual' on the International Law Applicable to Cyber Warfare, prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence DRAFT (as of August 21, 2012).
5. Michael Schmitt et al, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," Cambridge UK (Cambridge University Press), 2017.
6. Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," November 15, 2018; <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased>.
7. E.g., see Nicole Perlroth, "Online Security Experts Link More Breaches to Russian Government," October 28, 2014; <https://www.nytimes.com/2014/10/29/technology/russian-government-linked-to-more-cybersecurity-breaches.html> or Mark Johnson, "Russia Issues Travel Warning About US, Citing Threat Of 'Kidnapping'," IB Times, September 3, 2013, <http://www.ibtimes.com/russia-issues-travel-warning-about-us-citing-threat-kidnapping-1402265>.
8. Scott Charney et al, *From Articulation to Implementation: Enabling progress on cybersecurity norms*, June 2016.
9. *The Paris Call for Trust and Security in Cyberspace*, December 11, 2018; https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.
10. For a copy of the communique and a discussion thereof see Cody Poplin, "Cyber Sections of the Latest G20 Leaders' Communique," November 17, 2015; <https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communique>.
11. Adam Segal et al, *Hacking for CaSh: Is China Still Stealing Western IP?*, September 24, 2018; <http://apo.org.au/node/194141>.
12. Against China, see Ellen Nakashima, "Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyber-spying," Washington Post, May 22, 2014, http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb-9b59cde7b9_story.html; against Russia see "United States v. Viktor Borisovich Netyksho et al," Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18; <https://www.justice.gov/file/1080281/download>; against Iran see From Ellen Nakashima and Matt Zapotosky, "U.S. charges Iran-linked hackers with targeting banks, N.Y. dam," March 24, 2016; https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-government/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html.
13. The arrest and conviction of Karim Baratov is the closest to an exception; see David Shepardson, "Canadian who helped Yahoo email hackers gets five years in prison," May 29, 2018; <https://www.reuters.com/article/us-yahoo-cyber/canadian-who-helped-yahoo-email-hackers-gets-five-years-in-prison-idUSKCN1IU2OE>.
14. See David Frank Winkler, *The Cold War at Sea: High-Seas Confrontation Between the United States and the Soviet Union* (Annapolis, Md.: Naval Institute Press, 2000).
15. See Joseph Marks, "The Cybersecurity 202: These political candidates are running on their cybersecurity expertise," May 20, 2019; <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/20/the-cybersecurity-202-these-political-candidates-are-running-on-their-cybersecurity-expertise/5ce200171ad2e54b957e7fb2/>.
16. Max Smeets, "There are Too Many Red Lines in Cyberspace," March 20, 2019; <https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace>.
17. Matt Burgess, "North Korea's elite hackers are funding nukes with crypto raids," April 3, 2019; <https://www.wired.co.uk/article/north-korea-hackers-apt38-cryptocurrency>.
18. A similar argument can be made for Israel, which has carried out physical attacks in Syria and has been implicated in assassinations in Iran. Israel, technically and in some aspects practically, is at war with its neighbors. Again, such a justification means that its actions do not normalize operations in cyberspace for countries at peace.
19. Lily Hay Newman, November 28, 2018; "Russian Hackers Haven't Stopped Probing the US Power Grid," <https://www.wired.com/story/russian-hackers-us-power-grid-attacks/>.

NOTES

20. President Putin has compared those who hacked the DNC to “artists.” See Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," June 1, 2017; <https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html>.
21. Chris Demchak, Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs*, 3:1 (2018).
22. See, for instance, Scott Shane and Jonathan Weisman, "Earlier Denials Put Intelligence Chief in Awkward Position," June 11, 2013; <https://www.nytimes.com/2013/06/12/us/nsa-disclosures-put-awkward-light-on-official-statements.html>.
23. Considering oneself the gold standard has one obvious disadvantage. Any U.S. decision to do something that has never been done raises the question of whether doing so would give other the green light to do likewise. It is hard to believe that North Korea, Iran, Russian, and (for the time being) China make similar calculations.
24. Joseph Menn, "Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources," May 29, 2015; <https://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529>.
25. David Sanger and William Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," March 4, 2017; <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html>.
26. But if the United States is allowed to carry out cyberattacks on Iranian nuclear centrifuges could Pakistan or India use a similar rationale (“he did it first) to attack the other’s nuclear supply chain?”
27. For instance, see Ellen Nakashima and Joby Warrick, "For NSA chief, terrorist threat drives passion to ‘collect it all’," July 14, 2018; https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2018/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.
28. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," February 27, 2019; https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
29. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," June 15, 2019; <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
30. See, for instance, David Sanger, "Russian Hackers Appear to Shift Focus to U.S. Power Grid," July 27, 2018; <https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html>.
31. David Sanger, Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," February 16, 2016; <https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html>.
32. For instance, see Andy Greenberg, "The Highly Dangerous 'Triton' Hackers have Probed the US Grid," June 14, 2019; <https://www.wired.com/story/triton-hackers-scan-us-power-grid/>.
33. AFP, "US launched cyber attacks on Iran after drone shootdown: reports," June 22, 2019; <https://news.yahoo.com/us-launched-cyber-attacks-iran-drone-shutdown-reports-232123877.html>.
34. Not everyone thinks that gaining access against the IRGC (Islamic Revolutionary Guard Corps) would take that long given their state of cybersecurity.
35. "US and Russia clash over power grid 'hack attacks'", June 18, 2019; <https://www.bbc.com/news/technology-48675203>.
36. Alexandra Ma, "Iran says that US cyberattacks — said to be Trump's preferred retaliation — didn't work," June 24, 2019; <https://www.businessinsider.com/iran-us-cyberattacks-after-drone-shot-down-did-not-work-2019-6>.
37. For a more elaborated version of that argument, see the author's "Drawing Inferences from Cyber Espionage," Chapter 6 of the T. Minarik et al, 2018 10th *International Conference on Cyber Conflict*, Tallinn, Estonia (CCDCOE).
38. In other words, the United States would escalate its cyberspace activity for the express purpose of starting a process that yields de-escalation.
39. James Acton, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” *International Security*, 43: 1, 56-99.
40. Source: Sumi Somaskanda, "Germany's Cybersecurity Teams Fight 'Ticking Time Bombs'", June 23, 2018; <https://www.theatlantic.com/international/archive/2018/06/germany-cyberattacks/561914/>.

The Temporal Dimension of Defending Forward

A UK perspective on how to organize and innovate to achieve US Cyber Command's new vision

Alan Mears | Joe Mariani

ABSTRACT

The 2018 DoD Defense Strategy seeks to deter and defeat adversaries through a policy of forward engagement.^[1] The Strategy and the related USCYBERCOM Vision mark a significant change in how the US intends to contest the emerging complexity of cyberspace in an environment where the rules will be more restrictive for the US and its allies than those of adversaries. Recognizing an ingrained military culture of geographically driven maneuver warfare, it will be important that USCYBERCOM considers the temporal as well as the spatial elements required to defend forward. A combination of timely, better and more coherent decision making across a pan-government and industry ecosystem must exploit rather than attempt to control chaos; the effective adoption and application of decisive innovative capabilities will be a related essential element of this strategy. Through a UK lens, this paper considers the temporal implications of a strategy of Defending Forward.

INTRODUCTION

A body of recent U.S. Government publications has outlined a significant shift in strategic thinking in the context of the changing geopolitical climate and cyberspace; for example the 2018 U.S. National Defense Strategy states that adversaries no longer respect established global norms, and are engaged in a constant state of espionage, disruption and shaping activities against the US, and its allies.^[2] This is leading to increased competition across the full spectrum of Diplomatic, Information, Military and Economic (DIME) levers of national power. The UK's National Cyber Security Strategy and the International Institute for Strategic Studies (IISS) recognize the persistent and evolving cyber threat, manifested through such concepts as grey and tolerance warfare; these suggest that this emergent behavior is having an increasingly profound effect on our understanding of future threats to the prosperity and security of our nations.^{[3][4]}

© 2020 Alan Mears, Joe Mariani

Adversaries are aggressively exploiting policy and decision-making frictions and boundaries of the US and its allies.^[5] While this condition of constant competition falls short of overt conflict, it is all about out-maneuvering opponents. It is therefore essential that the US and the UK adapt their strategies and policies to both deter adversaries but also to seize and retain the initiative; Defend Forward should be approached as an active and not reactive strategy. Not to do so, or to do so too late, risks ceding the initiative entirely, as the Commander of U.S. Cyber Command (USCYBERCOM) has pointed out.^[6] The 2018 DoD strategy seeks to address this and directs the Department to defend forward, shape the day-to-day competition and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the Department and nation, cultivating talent, while at the same time actively competing against and deterring competitors.^[7]

Reflecting on this significant shift in emphasis, it is worth noting that much of the Defense community is culturally pre-disposed to apply positional context to operational problems. The traditional focus on maneuver tactics misses the importance of a campaign that shapes an adversary's political and economic networks to achieve a position of relative advantage.^[8] Thus Defend Forward and "close to the origins" may lead to a tendency to focus on the physical dimensions of the concept. If traditional physical boundaries such as Joint Operational Areas (JOAs) are now less relevant, it will be important to consider how other elements such as timely and accurate decision making and the ability to develop and maintain a winning edge in the application of innovative capabilities might contribute to this strategy.^[9] Against an understanding of related US and UK concepts and approaches being developed, this paper will consider some key temporal aspects that may contribute to the outcome of Defend Forward. Drawing on a review of available academic, policy and broader related literature, this paper will discuss the following:

- ◆ Briefly contextualize the requirement for Defend Forward
- ◆ Consider the temporal element as a contributing factor to Defend Forward
- ◆ Consider the role and possible approach to a coordinated pan-defense, government and industry trusted ecosystem
- ◆ Consider how concepts of anti-fragility and chaos might contribute to a decisive operating edge
- ◆ Analyze the key elements of the discussion to identify some key organizational principles and approaches that may contribute to the strategy of Defend Forward.

In considering these themes it is recognized that each is highly complex and worthy of more substantial analysis in their own right. The aim of this paper, however, is to introduce these as related themes to a broader audience in sufficient detail to demonstrate some key inter-dependencies and experiences that can contribute to the design and implementation of the future strategy.

DEFEND FORWARD IN CONTEXT

Military history demonstrates that the Commander who seizes and maintains the initiative dominates the adversary, and that defense properly conducted is a transitional phase that provides a platform for decisive effect.^[10] The Vision for USCYBERCOM, Achieve and Maintain Cyberspace Superiority, translates the National Defense strategy of Defend Forward into a cyberspace strategy of persistent engagement, a fundamentally new strategy for US cyber operations.^[11] The Defend Forward strategy will require cyber operators to seize and maintain the initiative in cyberspace by continuously engaging adversaries and causing them uncertainty wherever they maneuver. The strategy requires continual and global operations, keeping as close as possible to adversaries and their operations. A defense of this kind will create operational advantage for the US on the battlefield while denying the same to its adversaries.^[12] A number of significant implications are arising from this new approach that will need to be understood and addressed. Max Smeets highlights the degrees of collaboration and understanding the US will need to have with its allies if the US intends to conduct operations through or in their networks; there will be similar issues where these allies seek to operate over US networks.^[13] In addition, critics of Defend Forward question the efficacy of such a strategy which they see as increasing the risk of escalation while doing nothing to make cyber operations more effective.^[14]

As allies facing common trends, the UK thinking on cyber is moving in a similar direction to USCYBERCOM. While there is no direct UK Defence equivalent as yet to the USCYBERCOM Vision, the approach is well represented in a range of recent policies and approaches. The Joint Concept Note 2/18, Information Advantage, suggests that central to emerging strategic contests are “information battles” in which information is “weaponized” and where the UK and its allies increasingly lack the initiative.^[15] These require UK Defence, as part of a national and allied effort, to become a potent and resilient strategic actor postured for constant competition both at home and away. The developing Capstone Concept for Strategic Integration (CCSI) suggests that simply doing more of the same is not an option, and reinforces the need to drive the conditions and tempo of strategic activity, instead of merely reacting to the actions of others; the paper highlights the need to be agile and to operate at pace continuously developing new ways and means to compete.^[16] Similarly, reflecting the themes of the CCSI, the developing Integrated Operating Concept (IOpC) 2020 highlights the importance of a resilient home base as critical for any future operations, and the need for a unified and integrated cross-government Homeland Defence architecture to deliver this.^[17] In developing approaches to support these initiatives, the Army’s concept of Information Maneuver stresses the importance forward engagement and the power of the narrative in an era of Constant Competition; it recognizes warfare in the information age as a multi-domain battle which will face increasing challenges to its technical superiority requiring an agile acquisition and support network capable of responding to changing operational needs.^[18] Both the Royal Navy and the Royal Air Force are developing similar strategies; for example the Navy’s Project Nelson initiative is a dynamic

experimentation program looking at the application of a range of technologies such as AI and Machine Learning, and its approach to the adoption of autonomous systems is being seen as an exemplar in NATO.^[19]

Common to both US and UK visions for cyber operations is the requirement to stay consistently and continually engaged with networks, both social and physical, and problem sets beyond national borders. Naturally, this can lead to the idea that the new strategies simply expand the scope of cyber operations geographically, but the truth is that it also changes how cyber forces operate as well.

FORWARD IS TEMPORAL AS MUCH AS SPATIAL

Understanding and connecting the spatial and temporal elements of maneuver has been a critical element of the planning and execution of military operations throughout history. Given the global and instantaneous nature of the emerging cyberspace environment, connecting and exploiting the synergies of these elements will be an essential factor of Defend Forward. Untimely and poor decision-making can have profound implications for successful campaign outcomes. This does not necessarily require a faster Observe, Orientate, Decide, Act (OODA) loop, just the ability to act faster than the adversary which can be achieved by speeding up your own OODA loop, degrading that of the adversary, or more likely a combination of both. History provides multiple examples where appropriately forward-positioned forces have ended up in the wrong place through centralized or dysfunctional command and poor decision making. Reflecting on the 75th anniversary of D-Day, Allied success in Normandy, for example, was due in no small part to “fixing” forward-deployed, capable enemy formations in the wrong place through deception, sabotage and a lack of appropriately delegated authorities in the initial stages. Although the Germans were highly trained and skilled in counter-attack, they could not mount a successful defense.

Given the accelerating complexity and chaos of this environment, commanders will increasingly require flexibility and freedom, the agility to deal with rapidly changing demands. In these circumstances it may no longer be possible or even appropriate to plan or invest in the absolute detail of the layout or requirements of the future.^[20] At the same time, relying on rapid response and reactivity may place challenging, if not impossible, demands on capability, thus there is a related need to invest in anticipation. This is not a new concept in the military where it is an established truth that although a plan rarely “survives contact with the enemy” it is only through this process that real insight and agility can be derived.^[21] So the corollary of not having to react so quickly is that we have to take anticipatory steps much earlier, and shape activities to create the conditions under which problematic circumstances will either not arise, will be more benign, or can be more easily addressed.^[22] Commanders will therefore have to focus on creating the conditions, through appropriate policy frameworks and direction, under which their subordinates can operate.^[23] An important element of this approach will be the

ability of USCYBERCOM to not only accept, but to embrace, chaos. Dee Hock, former president of VISA International used the term chaordic to describe the need for organizations to be both chaotic and ordered to achieve agility.^[24]

Contributing significantly to this chaordic challenge is the added and perhaps unnecessary friction to timely decision making through the creation of the Fifth Domain of cyberspace.^[25] In doing this, the US, the UK, and their allies have created another, almost separate community that needs to be integrated and de-conflicted alongside the planning and orchestration of other closely related capabilities such as Electronic Warfare (EW), Psychological Operations (PsyOps), and Information Operations (IO). In contrast, Keir Giles states that Russia sees “information confrontation” or “information war” as a broad and inclusive concept which contains computer network operations alongside disciplines such as PsyOps, strategic communications, influence, intelligence, counterintelligence, deception, disinformation, electronic warfare, and destruction of enemy computer capabilities. Giles describes this as forming a “whole of systems” in which the blending and coordination between different informational tools is a distinctive feature of how Russia aspires to prosecute information warfare.^[26] The Chinese have a similar approach in their construct of Informationized Warfare.^[27]

While chaos may allow initiative to flourish, at the same time it should be held within a system of overall cooperation if it is to enable rather than confound.^[28] Across the Defense community the operational framework and the concept of Mission Command is designed to operate in such conditions that seek to combine subjective and objective behaviors to balance the art and the science of warfare.^[29] Mission Command has its origins in the 18th Century concept of *Auftragstaktik* within which the basic premise is that commanders should give subordinates general direction of what is to be done, allowing them the freedom to determine how to do it.^[30] This is reflected in the U.S. Army’s ADP 3-0 Unified Land Operations and ADP 6 Mission Command, Command and Control of Army Forces, which require Commanders to enable adaptive forces through flexibility, collaborative planning, and decentralized execution; Mission Command is seen to maximize autonomy and foster individual, initiative thereby enabling force elements to act rapidly through enhanced flexibility and adaptability across the range of military operations.^{[31][32]}

However, like any philosophy, Mission Command must be enabled if it is to deliver. In military operations, there is a growing tendency to limit initiative through overcentralized control and poor delegation. The ubiquitous nature of modern communications has further stifled Mission Command with strategic commanders able to tactically control the battle. This level of connectivity has also resulted in tactical actions that have much more of a strategic impact by being immediately visible to a global audience. In addition, the daily conduct of home based military activity does little to develop or foster the behaviors that underpin Mission Command; one has to question how the next generation of commanders will ever be comfortable with taking the responsibility such an approach requires when they are not routinely familiar with

its application. Despite these issues, Mission Command is still the advocated approach and one that is taught and recognized across Defense, but there is no such equivalent framework that embraces wider DIME community. Given these tensions between enabling initiative and centralized control across Defense, there are significant challenges and frictions that will confront any attempts to apply a Mission Command approach across the broader DIME ecosystem.

ENABLING AN ECOSYSTEM FOR DEFEND FORWARD

Recognizing the importance of US Critical National Infrastructure (CNI) and the broader public and private sectors as components of the strategy to Defend Forward, a key aim of the 2018 DoD Cyber strategy is the need to preempt, defeat, or deter malicious cyber activity targeting US CNI. It also highlights the need to provide public and private sector partners with Indications and Warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies. Given that conflict increasingly takes place across connected national societies that are inseparable from global networks, there are implications for militaries who depend on many of these networks as a minor user among many, thus opening up a Pandora's box of risks that now expose the very security and prosperity that Governments are investing in.^{[33][34]} Not surprisingly adversaries have observed the opportunities of this connectedness and also the increasing trend of elevating responsibilities and authorities to higher levels of command; they have recognized that the challenges and frictions of cross-government decision-making have made our systems comparatively slower and less agile.^[35] As former U.S. Secretary of Defense Ash Carter stated:

The State Department, for its part, was unable to cut through the thicket of diplomatic issues involved in working through the host of foreign services that constitute the Internet. In short, none of our agencies showed very well in the cyber fight.^[36]

This friction is reinforced by a lack of proportionate responses to deliberately escalating challenges which appear to be emboldening our adversaries.^[37] If today's organizing principle is no longer sovereign territory but a new geography and resulting geopolitics organized around social networks and supply chains then, as Martyn suggests, security will be based on a team effort that not only requires constant vigilance, but a community oriented, proactive mindset.^{[38][39]} A contributing feature in addressing this as identified by the Organisation for Economic Cooperation and Development (OECD) is the need for the wider diffusion of information among a larger number of workers. This increases the importance of management and co-ordination and the importance of a more horizontal work-based approach within digitally enabled workplaces. This requires teamwork rather than top-down management which in turn calls for more co-operation, collaboration and trust.^[40]

But the priorities of boards and directors of the majority of organizations across the public and private sectors are naturally driven more by compliance and profitability than National Security considerations; they may have little understanding of their evolving status as

potential targets for the political machinations of highly motivated and capable state-level actors, and even less for any additional expenditure on cyber defense which many view as a business loss.^[41] Engaging these organizations as part of a coordinated National Security effort within a Defend Forward ecosystem will require a more holistic and collaborative understanding of the shared risks, and the initiatives to address them. General Sir Richard Barrons observed that the ability to shake the foundations of a population’s morale and cohesion through skillful information-based manipulation means it is not always necessary to invade territory to break a state; this can be done decisively from long range, and he proposes an organizational structure to address this as illustrated at Figure 1.^[42]

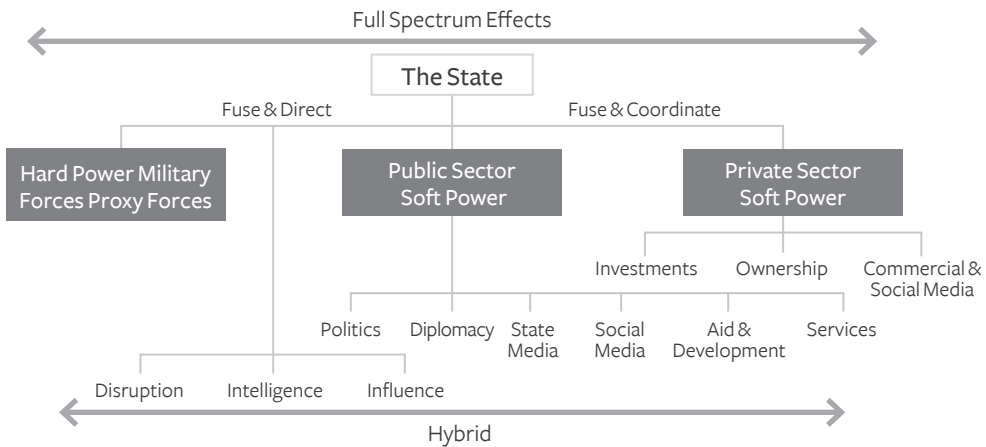


Figure 1: Success requires all levers of power ^[43]

UK efforts to address these particular challenges may provide some insights to USCYBERCOM. The development a new National Security doctrine, the Fusion Doctrine, is outlined in the National Security Capability Review (NCSR).^[44] This seeks to improve the UK’s collective approach to National Security and aims to use its security, economic and influence capabilities to maximum effect to protect, promote and project the UK’s national security, economic and influence goals. In particular the Doctrine notes that many of the capabilities that can contribute to National Security lie outside traditional National Security departments and also demand stronger partnerships between the public and private sector and the international dimension where security, trade and development partnerships are often mutually reinforcing. This Doctrine will play a key role in the UK’s approach to modern deterrence which will be conducted as a whole-of-government activity with the purpose of deterring catastrophic threats entirely.

There are significant cultural and organizational, as well as policy and technological challenges, which will need to be addressed within this strategy. Lacking the same immediacy of the threat as that for example perceived by the Baltic States, there is a limited appetite for the constraints and discipline necessary to deliver a policy of “Total Defence” to a population that is largely removed from the concept of the existential modern threat they face.^[45] It is therefore

evident that the complexity, and in many ways the near anarchy, of this complex ecosystem is unlikely to be addressed through an approach that relies on the rigid application of policies and statutes; the complexity and fluidity of the cyber domain combined with all of the social, cultural, organizational and legal challenges that are implicated will require the evolution of a DIME ecosystem that can orchestrate and enable the chaotic and anarchic nature of its components under a trusting and cohering purpose.

EXPLOITING ANTI-FRAGILITY AND CHAOS TO DELIVER AN OPERATING EDGE

Management science has known since at least the 1970s that faster, more responsive decision-making across complex organizations can result from delegation closer to the tactical edge, but this, in itself, creates its own tension as it is difficult to be sure that these decisions are coherent with the overall strategy.^[46] The traditional management approach is to have a strategy, break-out operational tasks, then distribute those tasks to subordinate tactical workers for execution. This allows tactical workers to be sure that their actions are coordinated and aligned to the outcomes the executives have pre-determined. Unfortunately, organizations competing at the pace of change in the modern world are discovering that such an approach results in poorer outcomes. While many executives may still create their strategic plans, they do this annually, at best, their workforce operating at the tactical edge must respond to changes in the environment on an almost daily basis as illustrated at Figure 2.^[47] This mismatch in the wavelength or periodicity of tasks at different levels stresses the structures of modern organizations and demands that decision makers be more agile.

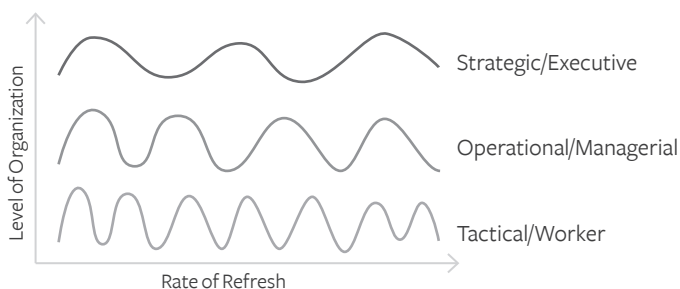


Figure 2: The “wavelength” of tasks in the modern world ^[48]

At the 2019 conference on Big Data for Defence in London the Chairman, General Andrew Sharpe, noted that:

“whatever the technology, procrastinators will still procrastinate, idiots will still be idiots. We must organize to be comfortable with chaos as we move forwards” .^[49]

A clear inference that can be drawn from this is that mental agility and dexterity will be an important personal characteristic of decision makers in an increasingly complex environment where organizations will need not only accept, but to embrace, chaos within a system of federation

and overall cooperation. Nassim Taleb suggests that complex man-made systems, such as the cyber domain, tend to develop runaway chains of reaction that decrease or even eliminate predictability causing outsized events. Paradoxically, the modern world, by increasing technological knowledge, is also making it more unpredictable.^[50] Taleb also suggests that a tendency to take the present as a baseline and then produce a speculative future based on the addition of technologies, although in some ways logical, tends to over technologize the approach adding further to the complexity, and thus the unpredictability, of the outcomes; instead he advocates the value of self-learning and gives weight to those elements that continue to survive.^[51] Taleb advocates the benefits of anti-fragility in the environment that is based around acceptance of the theory that corporate resilience derives from the recognition that federation is key and individuals are “unfit” components that should be allowed to fail if the corporation is to learn and progress. This approach, which encourages mistakes while also containing them, will succeed over one that tries to overcome failure through the over-centralization of control.^[52]

In the military context, in his book *Team of Teams*, General Stanley McCrystal reflects on many of these issues as he describes how his own experiences in Iraq and Afghanistan forced him to change as a leader and, in the process, find a new way of structuring and leading organizations in the chaos of the modern technological environment. Speaking to Joe Mariani, he observed that the tipping point for him was the realization that whereas previously only the military had access to the scale and complexity of resources that allowed decisive decision making over less well equipped adversaries, that technology had become widespread, and instant communication had become available to everyone.^[53] In addition, the sheer scale and complexity of data increasingly challenged attempts at sense-making within hierarchical and centralized Command and Control (C2) structures. What he discovered was the benefit of processing and exploiting information across the entire organization without tightly controlling that process, thus allowing everyone to think and have the information to allow them to act locally. The problem he faced with rapid change in the environment was the increased requirement for internal coordination or synchronization as the organization moved towards the chaotic as illustrated at Figure 3.

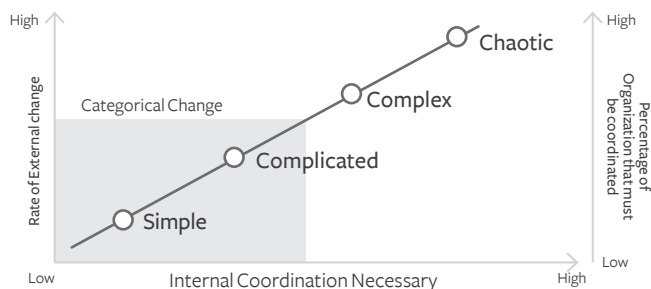


Figure 3: External change v Internal coordination^[54]

A key deduction he drew from this experience, and relevant to the complexity of modern persistent conflict, was the need to develop and work within a concept of trust and a common purpose to address the complexities and be adaptive. This approach should be based on shared consciousness and empowered execution which will allow the necessary speed and interdependence required for the “edge” elements to act quickly and independently but within the overall intent.^[55] This is illustrated at Figure 4.

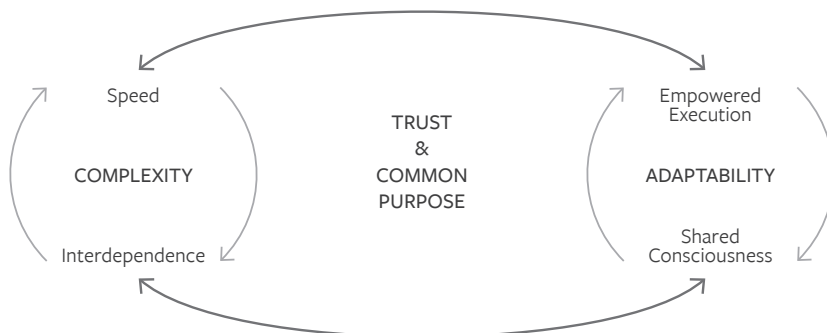


Figure 4: The role of Trust and Common Purpose in addressing complexity and chaos ^[56]

In the light of this discussion, it is evident that simply tinkering with current cultures and structures will be insufficient to deliver the vision of Defending Forward, and that a fundamental shift in organizational approach, culture and ethos will be required moving forward. Traditional notions that knowledge and wisdom are the preserve of the senior officer must adapt to a culture where leadership will embrace delegation, providing a cohesive vision. They should encourage and act in response to the advice and guidance of the most junior, non-commissioned junior officers and, where appropriate, non-military staff when they are clearly the experts.

DIFFERENT MISSIONS, DIFFERENT ORGANIZING PRINCIPLES

To understand how the issues discussed in this paper may inform future organizational constructs for USCYBERCOM, we need to understand the specific complexities that should be addressed as part of the new Vision. A deeper reading of the new Vision indicates that there are in fact different types of complexity and each one requires a different organizational structure. On the one hand, there is the need to constantly attend to the products and processes of the past, but at the same time, there is a need to explore the innovations that will define the future.^[57] The Vision intends to be able to conduct multiple tactical to strategic level operations concurrently, while there is valid debate over whether or not it is possible to separate out tactical, operational, and strategic levels of conflict today, it is reasonable to assume that tactical and strategic cyber operations start at two different ends of a spectrum but will have substantial overlaps. These two differing drivers and conditions largely set the tone of the effects required with different, if perhaps supporting, goals and means. With different

organizational forms being suited to different tasks, tactical and strategic offensive cyber may require different tools, teams, and structures to achieve the Defend Forward strategy. In order to execute these two concurrent missions, USCYBERCOM will need to organize to address two fundamentally different challenges concurrently: it will need agile cross-functional teams, enabled through a mechanism of delegation and trust combined with a common purpose to contest and succeed in today's fight and it will need to empower "practitioner" groups of planners and innovators, who will be plugged into large networks with the purpose of contesting and winning in the shaping and innovation space. This challenge of organizing to cover related but separate challenges is not uncommon in industry and is referred to as enabling the ambidextrous organization.^[58] On one hand, USCYBERCOM will need to become a now-focused, rapid response organization composed of cross-functional teams able to anticipate and respond tactically to any contingency. On the other hand, it will need to be a future focused organization with small groups strongly linked to innovators bent on developing technologies and techniques that will provide the operational edge.

Looking at former, the challenge of organizing to anticipate and respond rapidly to changing tactical circumstances is perhaps the best known of the two activities to a military audience. Acting faster than adversaries on land, air, and sea has been the backbone of decades of military strategies. But just because it is familiar does not mean that the answers are always immediately apparent even to the best trained and equipped units. The lesson from McChrystal and Joint Special Operations Command (JSOC) is that having the right strategy, the right tools and even the right people may not be enough if you are asking them to operate within a poorly designed system, and that organizational structures need to be tailored to the outcome that an organization's strategy demands.^[59] In order, therefore, to begin to organize to Defend Forward the key characteristics that will be required will need to include:

- ◆ Decision-makers with the necessary aptitude, mental agility and dexterity to understand and exploit opportunity
- ◆ Trust, a common purpose, and shared consciousness
- ◆ Delegated authorities and resources enabling the execution of operations to the edge
- ◆ Cross-functional teams focused on a common problem
- ◆ A focus on being a share-first organization to emphasize the flow of information between/among teams
- ◆ A change in the expectations of leaders from direct supervision to enablement
- ◆ An emphasis on developing a Mission Command orientated organizational culture so that leaders are more familiar with, and confident in, delegating to subordinates.

In turning to the latter, the strategic operations end of the spectrum, a temporal, maneuvering advantage can only be realized by achieving and sustaining a credible cyber advantage

over the adversary and his capabilities. This has the implicit task of requiring USCYBERCOM to remain permanently at the cutting edge of adopting and applying cyber related capabilities through empowered and delegated policies and decision making. For example in early 1943, (and strongly encouraged by Winston Churchill and supported by Chief of the General Staff and his brother-in-law General Montgomery) General Percy Hobart was put in charge of the newly formed 79th Armored Division to cohere a specialized armor innovation and operational adoption across a range of armored “funnies” to support the D-Day invasion—the rest, as they say, is history. There was no similar initiative in the US and this stovepipe mentality prevented the widespread dissemination of this specialized vehicle development theory, development and fielding until well after the war’s end.^[60] Hobart’s approach was one that was supported at the highest levels, had a cohering vision, and, while no idea was off the book, he took suggestions from all ranks.

While the National Defense Strategy states that:

success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting”, it is evident that today’s top down hierarchical approaches are not geared to this challenge.^[61]

The UK’s Future Force Concept identifies innovation, greater automation and creative thinking as keys to sustaining freedom of action in the emerging Operating Environment; it describes innovation as threatening existing capabilities in which militaries have made heavy investment and have cultural baggage.^[62] However, the evidence on both sides of the Atlantic points to long-established policies, cultures, processes, and structures that have a mixed record in facilitating rapid and innovative adoption, particularly in the areas of information technologies. Related to this, as identified by Klemas and Choucri, these frictions are further exacerbated by a struggling acquisition framework.^[63] These were far from fit for the late 20th Century, and unaddressed will become a growing inhibitor in the operating environment of the 4th Industrial Revolution.

What is increasingly advocated is a collaborative and interactive innovation mechanism that places knowledgeable operators at the center rather than at the beginning and end of a dispersed development process. In considering the applicability of Early Synthetic Prototyping (ESP), Smith and Vogt point to concept developers, capability developers, scientists, and engineers who continuously interact with the operator.^[64] This prototype of warfare concept will field many simple capabilities on a rolling basis, instead of a single, exotic one just once. Initially, a wide array of diverse prototypes will be developed and evaluated in experimentation programs. After, the particular prototypes that have proven successful in the trials will be produced in limited numbers and quickly introduced into service. A key element for success is the “Innovation Catalyst” who works within the senior leadership team and is demonstrably able to make change happen, and a fit for purpose and adaptive acquisition process.^[65]

Professor Nina Kollars puts forth a similar argument when she suggests that there is no innovation without adoption, suggesting adaptation is a key element of military innovation. There are many examples of innovative, battle-winning capabilities that were never realized, and which represent a rhetorical capability, rather than a real one. An understanding of the roles of Grand Design (the crazy ideas and the paradigm shifts), the nature of improvisation, and the role of experienced and insightful practitioners are key to innovative adoption. Practitioners form the anvil on which potential can be forged:

therefore, major military innovation requires the alignment of theory and practice—the marriage of the adaptation process with grand design.^[66]

In order to engender an environment in which this approach to innovation might flourish, Professor Kollars also suggests that innovation and its sub-processes need both chaos and structure. Paradoxically, this requires a balance of independent action, interconnectedness, and hierarchy to make it possible for all to enjoy its benefits; there is clearly some resonance here with the concepts of chaos discussed earlier in this paper.

In addition, for USCYBERCOM to gain and maintain a cutting edge over its adversaries, it should embrace the widest possible breadth of talent possible through innovative career structures and harnessing the diverse talent pool of the broader community through close connections with industry, academia and allies.^[67] These innovation hubs cannot be an ad-hoc, anarchic and a disconnected scattering of people across an organization. It will be critical that a constructive tension between a central brain and distributed and enabled hubs is realized through the appropriate connection between them and a shared understanding of a common purpose. The key characteristics that USCYBERCOM should therefore consider in addressing the right-hand temporal challenges to Defend Forward include the following:

- ◆ Anticipatory contingency planning to put in place the necessary enabling resources, policies and authorities and common purpose to enable rapid response
- ◆ Access to a wide range of talent
- ◆ A coherent, federated-but-connected innovation enterprise focused on exploiting the adaptability and adoption through practitioner-led participation; one that is plugged into the widest possible ecosystem of academics, industry, and allies possible
- ◆ Promotion of failure early in the process as a positive outcome to be rewarded
- ◆ An approach to live experimentation that develops and integrates the “good ideas” into adopted capabilities
- ◆ An agile and responsive and resourceful commercial and financial framework that delivers rapid prototype development and adoption within weeks as opposed to months or years.

CONCLUSION

The 2018 U.S. National Defense Strategy and the related USCYBERCOM Vision mark a significant change in how the US intends to contest the emerging complexity of cyberspace in an environment where the rules will be more restrictive for the US and its allies than for the adversary. The US should put in place the necessary conditions and capabilities that will enable the U.S. to overcome these constraints if it is to develop and maintain its advantage and Freedom of Action. Recognizing an ingrained military culture of geographically driven maneuver warfare, it will be important that USCYBERCOM considers the temporal as well as the spatial elements of its Forward Defense strategy. Using both a US and a UK lens, this paper has considered some of the temporal opportunities and challenges that can contribute to the strategy and suggested some cultural and organizational approaches that might help address them.

If the US and its allies are to learn from history, an approach that fails to recognize the temporal as well as the spatial factors will leave it dislocated and chasing shadows. They will need to realize that technological “advantage” is more a function of the application of “edge” capabilities through the faster adoption of winning solutions than simply the pursuit of new technologies. Enduring strategic advantage can only come from the close integration of process and technology and is driven largely by the manner in which practitioners, the people, are able to adapt to and integrate new capabilities. Since no individual organization can drive the development of every cutting-edge capability, USCYBERCOM should therefore look to place itself in an “innovation ecosystem.” This ecosystem should include broader government, industry, the public and US allies and partners. Building and reinforcing the necessary collaborative policies and behaviors to achieve this should be a priority for USCYBERCOM and the U.S. Government. Transforming traditional hierarchical approaches to innovation and acquisition towards a more federated, connected, and agile organization will be essential to the US and its allies, if they are to compete at the same pace, let alone faster, than their antagonists.

But most significantly of all, if the US is to remain inside the OODA loop of the adversary, which it must do, it will need to embrace chaos and enable its “edge” organizations to fight today’s fight within an understood and orchestrated strategy enabled by the necessary cultures, people, freedoms, and policies to act. Interestingly this is the very basis of Mission Command within the operational framework, a concept, which is more often than not, submerged under the constraining burdens of a lack of trust and risk-averse, centralized control.🛡️

Author Bios

Alan Mears

Alan Mears has over 40 years' service as a Regular and Reserve officer in the British Army and is an Associate Director in the UK Deloitte Cyber Security Risk Advisory team where most recently he filled an interim role as head of Cyber Security Assurance at Maersk. As an independent consultant he worked closely with the UK's Joint Force Cyber Group and the Cyber Joint User to develop the UK's MOD's Cyberspace Operations Ways of Working. In 2007 he set up the groundbreaking UK C2 Battlelab in Shrivenham where, working closely with deploying Brigades, he led efforts to "digitize" UK and NATO efforts into Afghanistan between 2007 and 2011. He was mobilized as SO1 Targets to IMEF for Operation Iraqi Freedom in 2003, and again to set up ISAF's Joint Fires and Targeting capability with HQ Allied Rapid Reaction Corps in 2006. Alan has an MSc in Cyberspace Operations from Cranfield University.

Joe Mariani

Joe Mariani leads research into defense, national security, and justice for Deloitte's Center for Government Insights. Joe's research focuses on innovation and technology adoption by both commercial businesses and National Security organizations. Joes' previous experience includes work as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

ACKNOWLEDGEMENTS

The authors thank the following for their contributions to this paper: Dr. Tel Venables of Tallinn University of Technology; Maj Gen Dr Andrew Sharpe CBE; Dr. Max Smeets of Stanford University; Jeremy Hilton; Cranfield University; Brendan Kober.

NOTES

1. Department of Defense, Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge, available at: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
2. Ibid.
3. United Kingdom National Cyber Security Strategy 2016-2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
4. IISS Strategic Survey 2018: The Annual Assessment of Geopolitics, Routledge, 2018.
5. Department of Defense Strategy for Operations in the Information Environment, P4, June 2016.
6. General P. Nakasone, A Cyber Force for Persistent Operations, JFQ 92 January 2019, available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.
7. Department of Defense, Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge, available at: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
8. Charles Cleveland, Benjamin Jensen, Arnel David, and Susan Bryant, Military Strategy for the 21st Century People, Connectivity, and Competition. Rapid Communications in Conflict and Security Series General Editor: Geoffrey R.H. Burn, Cambria Press New York.
9. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed., "The Future Conflict Operating Environment Out to 2030," <https://rusi.org/publication/occasional-papers/future-conflict-operating-environment-out-2030>.
10. Maj Gen (Dr.) Andrew Sharpe. Discussion with the author Jul 16, 2019.
11. Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority: <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.
12. Ibid.
13. Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Lawfare Blog (2019): <https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies>.
14. Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," CATO Institute Policy Analysis No. 862, January 2019, available at: <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>.
15. UK MOD, Joint Concept Note (JCN) 2/18, Information Advantage, November 2018, available at: <https://www.gov.uk/government/publications/information-advantage-jcn-218>.
16. The Capstone Concept for Strategic Integration (CCSI) The Defence Contribution as at February 2019.
17. Integrated Operating Concept (IOpC) 2020, September 3, 2019.
18. British Army Information Manoeuvre Conemp 2019.
19. Colonel Dan Cheesman, Chief Technology Officer, Royal Navy, IQPC Disruptive Technologies Conference, London, September 25, 2019.
20. Lorraine Dodd and Geoff Markham, "C2 Agility, Different Models of Change and Reasoning with Time," 17th ICCRTS: "Operationalizing C2 Agility" Paper 014, 2012.
21. Daniel J. Hughes and Harry Bell. Moltke on the Art of War: Selected Writings, 1993, 92.
22. Ibid.
23. Ibid.
24. Lee Dyer and Richard A. Schafer, "From Human Resource Strategy to Organizational Effectiveness: Lessons from Research on Organizational Agility," Centre for Advanced Human Resource Studies, Working Paper, (1998).
25. U.S. Joint Chiefs of Staff Joint Publication 3-12(R), Cyberspace Operations.
26. Keir Giles, NATO Handbook of Russian Information Warfare, Fellowship Monograph, Rome: NATO Defense College, 2016.
27. Timothy L. Thomas, Dragon Bytes: Chinese Information-War Theory and Practice, Ft. Leavenworth, KS: Foreign Military Studies Office, 2004.
28. Philip Boxer, "Working on the Edges," in *Asymmetric Leadership*: <http://www.asymmetricalleadership.com/category/centre-vs-edge>.

NOTES

29. AJP-5, Allied Joint Doctrine for the Planning of Operations (Edition A), NATO Standardization Office, 2019.
30. John T Nelsen II, "Auftragstaktik: A Case for Decentralized Battle," *Parameters*, September 1987.
31. ADP 3-0 Unified Land Operations, Headquarters Department of the Army, 2011.
32. ADP 6 Mission Command: Command and Control of Army Forces, July 31, 2019
33. Myriam Dunn Cavelty, "Cyber-Security and Threat Politics" in *CSS Studies in Security and International Relations*, London, New York: Routledge, 2008.
34. Jose Nazario, "Politically Motivated Denial of Service Attacks," *Cryptology and Information Security Series 3, The Virtual Battlefield: Perspectives on Cyber Warfare*, Clifton: IOS Press, 2009, 163-181.
35. James E. McGhee. *Liberating Cyber Offense*. *Strategic Studies Quarterly*, Winter 2016, available at https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-4/McGhee.pdf.
36. Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," Belfer Center for Science and International Affairs, Harvard Kennedy School Report, 2017.
37. "Tolerance Warfare," IISS Strategic Survey 2018: The Annual Assessment of Geopolitics, IISS, 2018.
38. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed, "The Future Conflict Operating Environment Out to 2030".
39. P. Martyn, *Risky Business: Cybersecurity And Supply Chain Management*, Forbes, 2017, available at: <https://www.forbes.com/sites/gradsoflife/2017/08/18/more-than-whats-on-paper-how-gaining-independence-created-a-pathway-to-success/#299b02e11c14>.
40. Organisation for Economic Cooperation and Development (OECD) and Mohammed Bin Rashid Centre for Government Innovation, *Embracing Innovation in Government Global Trends 2017*, Paris, OECD, February 2017.
41. Ibid.
42. General Sir Richard Barrons, note to Alan Mears, November 2018.
43. Ibid.
44. UK Government, *National Security Capability Review*, London: Cabinet Office, 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.
45. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed., "The Future Conflict Operating Environment Out to 2030," 2019, 9.
46. Herman Vantrappen and Frederic Wirtz, "When to Decentralize Decision Making, and When Not To," *Harvard Business Review*, December 2017.
47. Joe Mariani, "Leading to Chaos: A Conversation with General Stanley McChrystal," *Deloitte Review* 19, July 2016 available at: <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/general-stanley-mcchrystal-interview-innovation-in-leadership.html>.
48. Ibid.
49. Major General (Ret.) Andrew Sharpe, Opening Remarks, Defence IQ Big Data for Defence Conference, London, June 25, 2019.
50. Nassim Nicholas Taleb, *Antifragile: Things that Gain from Disorder*, New York: Penguin Random House LLC, 2012.
51. Ibid, 313-315.
52. Ibid, 65-80.
53. Joe Mariani, "Leading to Chaos: A Conversation with General Stanley McChrystal," *Deloitte Review* July 19, 2016, available at: <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/general-stanley-mcchrystal-interview-innovation-in-leadership.html>.
54. Ibid.
55. Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World*, New York: Portfolio Penguin, 2015.
56. Ibid.
57. Charles A. O'Reilly III and Michael L. Tushman, "Innovation: The Ambidextrous Organization," *Harvard Business Review* (April 2004): <https://hbr.org/2004/04/the-ambidextrous-organization>.
58. Ibid.

NOTES

59. McChrystal, *Team of Teams*.
60. Major Michael J. Daniels, *Innovation In The Face Of Adversity: Major-General Sir Percy Hobart and the 79th Armoured Division (British)*, Pickle Partners Publishing, 2015.
61. Department of Defense, *Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge*.
62. UK MOD, *Joint Concept Note (JCN) 1/17, Future Force Concept*, September 2017: <https://www.gov.uk/government/publications/future-force-concept-jcn-117>.
63. Thomas Klemas, Nazli Choucri, Cyber Acquisition Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace, CYCON US 2018, available at: <https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session2-Paper3.pdf?ver=2018-11-13-160900-057>.
64. Dr. Robert Smith and Brian Vogt, "Early Synthetic Prototyping Digital Warfighting For Systems Engineering," *Journal of Cyber Security and Information Systems* Volume 5 no., December 4, 2017.
65. Thomas Klemas, Nazli Choucri, Cyber Acquisition Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace. USCYCON 2018, available at: <https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session2-Paper3.pdf?ver=2018-11-13-160900-057>.
66. Professor Nina Kollars, "Innovation is an Illusion," TEDx talk, Franklin & Marshall College, June 2016, <https://www.youtube.com/watch?v=9UpAl0rmQ7o>.
67. R. S. Burt, Martin Kilduff, and Stefano Tasselli, "Social Network Analysis: Foundations and Frontiers on Advantage," *Annual Review of Psychology* 64, 2013, available at: <https://faculty.chicagobooth.edu/ronald.burt/research/files/SNA.pdf>.

Defending Forward on the Korean Peninsula

*Cyber Deterrence
in the U.S.-ROK
Alliance*

Dr. James E. Platte

ABSTRACT

The United States has provided extended deterrence, backed by U.S. nuclear weapons, to South Korea since the end of the Korean War in 1953, and despite repeated low-level provocations by North Korea, the U.S.-ROK alliance has successfully deterred strategic attack on South Korea. The allies now face a growing asymmetric threat from North Korea in the cyber domain, and the alliance has yet to incorporate the cyber domain into the allied strategic deterrence posture. This paper examines cyber deterrence thinking and analyzes how to formulate a cyber deterrence posture as part of the overall strategic deterrence posture of the U.S.-ROK alliance. As with kinetic attacks, the alliance should focus on deterring cyber-attacks that produce cross-domain strategic effects and divide responsibilities to leverage each other's capabilities and interests. Even for cyber-attacks that do not reach the threshold of producing strategic effects, U.S. Defense Department cyber concepts like "defending forward" and "persistent engagement" can be operationalized to reduce the threat to South Korea posed by the range of North Korea's malicious cyber activity.

I. INTRODUCTION

The alliance between the United States and the Republic of Korea (ROK, otherwise referred to as South Korea) has evolved significantly since the two countries signed a mutual defense treaty in 1953. Geopolitical changes since 1953, particularly the collapse of the Soviet Union and the economic rise of East Asia, have driven many of the changes in the alliance, but technological changes also have significantly impacted the alliance. The digital revolution and the penetration of digital technologies throughout all facets of society has led to the U.S.-ROK alliance placing an increased emphasis on dealing with threats in the cyber domain. This paper will analyze how the two allies view cyber deterrence and how theories of deterrence can be applied to the cyber domain in the context of the U.S.-ROK alliance.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

While the U.S.-ROK alliance has “has expanded into a deep, comprehensive global partnership,” the core of the alliance remains defending South Korea from North Korean aggression.^[1] The joint communique from the U.S.-ROK Security Consultative Meeting in October 2018 reaffirmed this point by stating the fundamental mission of the alliance is “to defend the ROK through a robust combined defense posture and to enhance the mutual security of both nations under the U.S.-ROK Mutual Defense Treaty.^[2] This paper will focus on how the allies can approach deterring and defending cyber threats to South Korea, particularly threats originating from North Korea. There will be an implicit focus on the two militaries’ roles in cyber deterrence, but with an acknowledgement that cyber deterrence, like other forms of deterrence, requires a whole-of-government approach.

From a theoretical perspective, much of the deterrence thinking will come from the nuclear era, even though the concept of deterrence is likely as old as international relations and has roots in criminology and other non-military fields. Yet, much of the contemporary thinking on deterrence, especially in the US, comes from the superpower showdown between the Soviet Union and the US during the Cold War. Scholars have described four waves of deterrence research in the nuclear era, and there has been much scholarly and policy work done on developing cyber deterrence theories in recent years.^[3] But as Joseph Nye noted in 2017, “[t]heorizing about deterrence in the cyber era is emerging from only its first wave.”^[4] Thus, this paper also will explore how theories of deterrence from the nuclear era can apply in the cyber domain, with a focus on cyber deterrence in the U.S.-ROK alliance context.

The second section of this paper will give an overview of deterrence theory and general methods of deterrence. Next, section three will discuss who and what is to be deterred in the cyber domain by the United States and South Korea and how cyber deterrence compares to other deterrence domains in the U.S.-ROK alliance. The fourth section will examine what has been said, so far, regarding cyber deterrence by the US and South Korea. Then section five will analyze how different methods of deterrence could be applied to bolstering deterring cyber threats to South Korea. The paper will conclude with thoughts on deterrence theory in this alliance relationship and with policy recommendations for the U.S.-ROK alliance.

II. OVERVIEW OF DETERRENCE THEORY AND METHODS

Concepts of deterrence in international relations literature can be found at least as far back as the Peloponnesian War.^[5] The most common conception of deterrence can be described as dissuading an adversary from taking an action by threatening unacceptable violence in retaliation. This definition of deterrence has been come to be known as deterrence by punishment or deterrence by retaliation and was the most dominant form of deterrence thinking during the Cold War, elucidated by such prominent scholars as Thomas Schelling and Herman Kahn.

The overwhelming destructive power of nuclear weapons led scholars and practitioners to focus on deterrence by punishment from the start of the nuclear age. The retaliatory power

of nuclear weapons made war nearly unthinkable to many early deterrence scholars, and any instance of deterrence failure in the nuclear era was unacceptable. In 1946, Bernard Brodie famously summarized this sentiment, declaring “[t]hus far, the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them.”^[6] Other prominent deterrence scholars, including Schelling and Kahn, similarly espoused a strategy of deterrence based on the overwhelming power of nuclear weapons.

However, deterrence can be applied more broadly than this punishment model. In addition to deterrence by punishment, Glenn Snyder proposed another concept termed deterrence by denial in the late 1950s. Snyder viewed deterrence strategies as manipulating an adversary’s cost-benefit analysis, and deterrence “means discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing prospective gain.”^[7] Whereas deterrence by punishment acts on an adversary’s estimate of possible costs, deterrence by denial acts on an adversary’s estimate of the probability of gaining benefits. Thus, as Jeffrey Knopf observed, “denial strategies aim to dissuade a potential attacker by convincing them that the effort will not succeed and they will be denied the benefits they hope to obtain.” Combining these two concepts of deterrence into a more robust definition, Joseph Nye provided a broader definition of deterrence as “dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.”^[9]

Inherent in both of these concepts of deterrence is that deterrence occurs in the mind of an adversary. Deterrence is a function of the defender’s capability and will to punish or deny, and the defender can formulate and signal a strategy to deter an adversary. But more appropriately, deterrence occurs as a function of an adversary’s belief in the defender’s capability and will to punish or deny. Deterrence scholars emphasize that the credibility of the defender’s deterrence posture and effectively signaling this posture to an adversary is essential for creating a deterrent effect in the mind of an adversary. Recognizing that deterrence is a psychological phenomenon, scholars such as Robert Jervis, Richard Neb Lebow, Janis Stein, and Jeffrey Berejikian analyzed the effect that bias, misperception, and other cognitive functions can have on the success or failure of deterrence.^[10] Nye summed up their arguments by stating, “[d]eterrence is a psychological process that depends on the perceptions of both the actors and the targets, and the ability to communicate those views clearly.”^[11]

Nye also adds two methods of deterrence to this discussion: deterrence by entanglement and deterrence by norms. Nye defines entanglement as “the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim.”^[12] These interdependences, either dyadic or systemic, can lead a state to perceive that there is more benefit to maintaining the status quo than to potentially upsetting the status quo through some form of attack, even if the attack is not defended against or there is no fear of retaliation.^[13] Deterrence by norms works “by imposing reputational costs that can damage an actor’s soft power beyond the value gained from a given attack. Like entanglement, norms can impose costs on an attacker even if the attack is not denied by defense and there is no retaliation.”^[14]

Just like the concept of deterrence itself, none of these four methods of deterrence are exclusive to the nuclear domain or are inherently tied to nuclear weapons. Deterrence and the different deterrence strategies can apply to all domains, but there are challenges to applying each of these four deterrence methods in the cyber domain. The optimal cyber deterrence strategy likely will require a combination of these methods, and creative deterrence thinking will be required to move deterrence theories beyond the nuclear domain.

III. WHO AND WHAT TO DETER IN THE CYBER DOMAIN

The first step to crafting a cyber deterrence strategy is to answer the following two questions. First, who is being deterred, and second, what action is being deterred? Since this paper focuses on the U.S.-ROK alliance, answering those two questions requires identifying who are the major actors that threaten South Korea in the cyber domain.

The 2018 U.S. Department of Defense (DoD) Cyber Strategy identifies four states that employ malicious cyber activities to threaten US interests: China, Russia, Iran, and North Korea.^[15] While those four states and non-state actors could employ cyber threats against South Korea, the ROK Ministry of National Defense's (MND) 2016 Defense White Paper only calls out North Korea.^[16] Cybersecurity scholar Donghui Park also wrote that South Korea's primary external cyber security challenge is cyber attacks from North Korea.^[17] Thus, for this paper, the answer to who is to be deterred is North Korea.

Answering what is to be deterred is not quite as straightforward as just cyber-attacks against South Korea originating from North Korea. But before attempting to formulate a more nuanced answer as to what is to be deterred, an additional point on deterrence theory should be made here for the U.S.-ROK alliance. For South Korea, this discussion involves direct deterrence, which concerns actions against one's own state and its immediate interests. The US provides extended deterrence, which is "dissuasion of adversary actions against a third party or non-immediate interests," for South Korea.^[18] This distinction is fairly clear in the nuclear domain, where the US extended deterrence guarantee is meant to deter nuclear attack on South Korean territory, and US direct deterrence is meant to deter nuclear attack on U.S. territory. The interconnected nature of the cyber domain does not make the distinction between direct deterrence and extended deterrence as clear. US and South Korean interests can easily overlap in the cyber domain, and attacks on networks or digital systems that are owned and controlled by South Korean entities can have significant impacts on US interests, too.

In addition to this blurring of direct deterrence and extended deterrence in the cyber domain, there also is a wide range of malicious cyber behaviors that are undesirable, and it is not realistic to expect that the U.S.-ROK alliance can and should aim to deter the entire spectrum of malicious cyber behavior that could be directed at South Korea. Comparing the U.S.-ROK alliance's deterrence posture in other domains, namely nuclear and conventional, could be a useful starting point for thinking of where cyber deterrence fits into the alliance's overall deterrence posture and what actions are to be deterred in the cyber domain.

The original mutual defense treaty between the United States and the Republic of Korea signed in 1953 only briefly mentions deterring “armed attack” but does not elaborate further on who and what is to be deterred by the alliance.^[19] There is a wide range of acts that could be considered armed attack, but more recent statements by the allies provides some more clarity. The joint communique from the 2017 U.S.-ROK Security Consultative Mechanism (SCM), an annual meeting between the US Secretary of Defense and the ROK Minister of National Defense, proclaimed that the United States would provide extended deterrence “using the full range of military capabilities, including the US nuclear umbrella, conventional strike, and missile defense capabilities.”^[20] The allies also committed to strengthening their “deterrence measures and capabilities in response to the increasing North Korean nuclear, weapons of mass destruction (WMD), and ballistic missile threat.” The joint communique from the 2018 SCM reiterated the U.S. extended deterrence commitment from the previous year and added that the U.S.-ROK Combined Forces Command “has played the central role in deterring war on the Korean Peninsula” since it was formed in 1978.^[21]

The allies have increasingly focused on the threat from North Korea’s nuclear, WMD, and ballistic missile programs in recent years, most notably establishing a joint Tailored Deterrence Strategy Against North Korean Nuclear and other WMD Threats in 2013. This strategy created a framework for “tailoring deterrence against key North Korean nuclear threat scenarios across armistice and wartime.”^[22] Joint communiqués from subsequent SCMs all have mentioned implementing the Tailored Deterrence Strategy, making it a major pillar of the U.S.-ROK alliance. At the press conference announcing the signing of the Tailored Deterrence Strategy, then-ROK Minister of National Defense Kim Kwan-jin added that the U.S.-ROK alliance “has efficiently deterred North Korean provocations, as well as maintained peace and stability on the Korean peninsula.”^[23]

It also is worth considering what providing extended deterrence means for the United States. Extended deterrence may be most commonly thought of as using U.S. nuclear weapons to deter nuclear attack on U.S. allies, but the 2018 Nuclear Posture Review (NPR) made clear that the United States does not reserve using its nuclear weapons only for deterring other nuclear weapons. The NPR stated that the United States “would only consider the employment of nuclear weapons in extreme circumstances. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.”^[24] Thus, U.S. nuclear weapons are used for deterring all strategic attacks, both nuclear and non-nuclear, and the 2018 NPR also commits the United States to deterring strategic attacks on its allies.

Taken together, the recent SCM joint communiqués, the Tailored Deterrence Strategy, and the 2018 NPR imply that the US extended deterrent commitment to South Korea is intended

to deter strategic attacks on South Korea. Strategic attacks could include North Korean use of nuclear, biological, or chemical weapons or a large-scale, conventional attack on South Korea. Attacks or provocations that fall below the strategic level may be included more in the U.S.-ROK alliance’s defense posture, or the South Korean military may take primary responsibility for deterring and defending against non-strategic attacks and provocations.

The history of the U.S.-ROK alliance also suggests that this division of responsibilities between the allies is the case. North Korea has conducted repeated attacks and provocations against South Korea, occasionally resulting in South Korean casualties or destruction of property, but the US preference after such provocations has been to deescalate and restore deterrence before escalating to a larger conflict. No North Korean provocation since the invasion that started the Korean War on 25 June 1950 has risen to the level of strategic attack. Despite numerous North Korean provocations, this is why the allies can credit the U.S.-ROK alliance with preserving peace on the Korean Peninsula since hostilities in the Korean War ceased in July 1953. This also is an implicit acknowledgement of the difficulty of deterring lower-level provocations, especially against a determined adversary like North Korea.



Figure 1. Division of responsibility for deterring North Korean kinetic attacks on South Korea

Figure 1 graphically summarizes this deterrence posture of the U.S.-ROK alliance. On the full spectrum of kinetic attacks that North Korea could launch against South Korea, the U.S.-ROK alliance takes more responsibility at the upper end, and South Korea takes more responsibility at the lower end, represented by so-called gray zone attacks. The U.S.-ROK alliance certainly could have a deterrent effect on lower-level attacks, but the alliance is postured more toward deterring strategic attacks.

One could reasonably project that the U.S.-ROK alliance would posture similarly in the cyber domain. Namely, South Korea would take more responsibility for deterring lower-level North Korean cyber provocations, and the U.S.-ROK alliance would take more responsibility for deterring strategic cyber-attacks. This is depicted in Figure 2.



Figure 2. Division of responsibility for deterring North Korean cyber attacks on South Korea

The bigger challenge then is determining what constitutes a cyber-attack with strategic effect or what types of cyber-attacks the U.S.-ROK should posture to deter. The following list provides

examples of North Korean cyber-attacks on South Korean entities.^[25] This list is not comprehensive but gives some of the more impactful North Korean cyber-attacks. North Korea's cyber-attack on Sony Pictures in 2014 is not included because that attack targeted U.S. entities.

- ◆ July 2009: Distributed denial of service (DDoS) attack on US and ROK websites, including Blue House and White House, destroyed nearly 1,500 computers
- ◆ April 2011: Attack on Nonghyup Bank that deleted financial data from 273 servers that disrupted financial networks for 20 days
- ◆ March/June 2013: DarkSeoul attacks on ROK media, financial firms, and Blue House servers that destroyed some 48,000 computers and servers at 68 institutions
- ◆ December 2014: Hack of Korea Hydro and Nuclear Power released nuclear reactor data, including a power plant blueprint
- ◆ September 2016: Attack on ROK MND vaccine server and theft of U.S.-ROK planning documents^[26]

For the U.S.-ROK alliance, the first question to ask when looking this history of North Korean cyber-attacks on South Korea is whether any of them are the type of attack against which the alliance needs to posture to deter. It is arguable that none of these attacks had strategic effects on South Korea, but the diversity of targets and increasing scale of damage is concerning. It also is less clear in the cyber realm what type of attack would produce strategic effects, especially since cyber attacks could be used as a precursor to or force multiplier for larger-scale kinetic attacks.

In the cyber domain, South Korean scholars write that North Korea's primary aim is "to attack the intelligence network when there is a total war to delay the intervention of U.S. troops."^[27] This cyber operation would then be followed by attacking South Korea's C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) system to neutralize ROK weapon systems and munitions support, which would leave South Korean troops vulnerable to massive kinetic attacks. Another South Korean scholar speculated that North Korea could "first conduct a simultaneous and multifarious cyber offensive on...society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons."^[28] While the cyber-attacks listed above are concerning and require some sort of response, the potential for combining cyber-attacks with conventional or nuclear weapons is more troubling for the U.S.-ROK alliance.

Along the lines of the hybrid attack scenarios described by scholars, South Korea's 2016 Defense White Paper also suggested what should be the focus of an alliance cyber deterrence posture. "To prepare for potential cyber-attacks from North Korea, a framework for protecting critical national infrastructures and military-operated systems is currently under development."^[29] Cyber attacks on South Korean critical infrastructure or military networks have

the most potential to produce strategic effects, either on their own or when combined with conventional or nuclear weapons, and North Korea could use various cyber tools to attack ROK critical infrastructure or military networks.

Thus, the U.S.-ROK alliance should focus on deterring North Korean cyber attacks that have strategic effects or could enable strategic attacks, not particular types of cyber weapons or attacks. This cyber deterrence posture should include ROK critical infrastructure, military C4ISR and warning systems, and systems critical for network-centric warfare. The December 2014 hack of South Korea's nuclear plant operator and September 2016 hack of ROK MND servers could be examples of attacks that the alliance should posture to deter in the future, although neither of those attacks on their own produced strategic effects. The lack of clarity on the effects of cyber attacks is a significant issue that the alliance will have to grapple with when making a cyber deterrence strategy. South Korea should take whole-of-government approach to deter, defend, and respond to lower level attacks, such as those on ROK government websites, South Korean financial and media companies, and DPRK information operations.

This is not to say that the alliance should not be concerned with malicious North Korean cyber activity that falls below the threshold of producing strategic effects. As with kinetic attacks, lower level cyber attacks are disruptive and damaging to South Korean society, threaten US personnel and interests in South Korea, and can damage the credibility of the US security commitment in the minds of South Koreans. This is where the United States can operationalize its "defending forward" and "persistent engagement" concepts to help South Korea address lower level North Korean cyber attacks.

As the vision statement for U.S. Cyber Command (USCYBERCOM) declares, "Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace."^[30] In this way, the U.S.-ROK alliance can act against sub-strategic threshold North Korean attacks to both counter those attacks and possibly produce a deterrent effect against similar attacks in the future. North Korea is notorious for not accepting or upholding norms of behavior, but persistent engagement could compel North Korea to at least respect U.S.-ROK norms in the cyber domain.

Defending forward and persistent engagement are also similar to the concept of cumulative deterrence, which Israel has developed to address threats from non-state actors. Cumulative deterrence simultaneously uses "threats and force (mostly military) over the course of an extended conflict."^[31] By employing force and achieving a series of victories accumulated over extended periods, the defender moderates the behavior of the adversary, which leads to the adversary reducing the scope, scale, or frequency of attacks.^[32] Reducing the scope, scale, and frequency of lower level North Korean cyber attacks through active defense and deterrence also should be an objective of the U.S.-ROK alliance.

Ideally, the U.S.-ROK alliance or South Korea on its own could formulate a cyber deterrence posture that would prevent all such attacks in the future, but as with kinetic attacks, not all cyber attacks can be deterred. North Korea also seems to have embraced the cyber domain and sees cyber operations as being able to achieve tactical, operational, and strategic objectives during peacetime and in war.^[33] North Korea is a very determined cyber actor, and it may be difficult to deter lower-level attacks, just like it has been difficult to deter lower-level conventional attacks by North Korea. South Korea can focus on defending, responding to, and recovering from lower-level attacks, and the U.S.-ROK alliance can focus on deterring strategic or potentially strategic attacks from North Korea.

IV. U.S.-ROK VIEWS ON CYBER DETERRENCE

In order to posture to deter cyber-attacks that could have strategic effects, the allies need to express their ability and willingness to deter such attacks, but there has been no comprehensive U.S.-ROK cyber deterrence statement or document released. The allies have made several joint statements on cooperation in the cyber domain, and both the United States and South Korea have made their own statements related to cyber deterrence. This section will examine some of the major statements regarding the cyber domain to see where the U.S.-ROK alliance stands in crafting a cyber deterrence posture.

This section will focus on statements since the start of the Trump administration in 2017 (current ROK President Moon Jae-in also assumed office in 2017), but setting a baseline for those statements is a 2015 joint statement on the U.S.-ROK alliance made by the previous US and South Korean presidents. That 2015 statement gave four areas of emphasis for U.S.-ROK alliance cooperation in cyberspace:

- 1) enhancing information sharing on cyber threats, particularly to critical infrastructure,
- 2) strengthening collaboration on investigation on cyber incidents,
- 3) deepening military-to-military cyber cooperation, and
- 4) encouraging collaboration on cybersecurity research and development, education and workforce development, and cooperation on technology between cybersecurity industries.^[34]

The US and South Korea also pledged to strengthen bilateral cooperation mechanisms, including the U.S.-ROK Cyber Policy Consultations and the mil-to-mil Cyber Cooperation Working Group, and they established a White House-Blue House cyber coordination channel.

This statement does not mention deterrence specifically and lacks much detail, but there is a focus on protecting critical infrastructure and military networks. Importantly for deterrence, there also is a focus on identifying threats and the source of an attack. The attribution problem is widely recognized in the cyber domain, and a deterrent threat cannot be carried out if the attacker is not identified in a timely manner.

On the military side, the SCM joint communiqués provide even less detail on how the U.S.-ROK alliance views cyber deterrence. The 2017 SCM joint communiqué “recognized cyber capacity as a core security issue and decided to expand bilateral defense cooperation in cyber-related areas. Through regular bilateral engagements and the ROK-U.S. Cyber Cooperation Working Group (CCWG), both sides plan to continue to explore new opportunities to enhance cooperation.”^[35] The 2018 SCM joint communiqué struck a similar tone, with the allies committing to “strengthen Alliance cyber capabilities in light of the increasing scope of cyber security threats...share information regarding the reorganization of their respective cyber commands in order to promote cyber security cooperation in the future.”

These statements show that the US and South Korea both recognize that the cyber domain is increasingly important to the alliance, but there is little detail on how the U.S.-ROK alliance plans to develop a joint cyber deterrence posture. The last sentence quoted above from the 2018 SCM joint communiqué shows a problem that the alliance faces in crafting a joint cyber deterrence strategy. Both countries are still developing their own strategies, policies, and organizations to address the cyber domain, which complicates developing joint cyber strategies, policies, and operations necessary to create an effective joint cyber deterrence posture.

The U.S. Department of State released major cyber policy documents in 2016 and 2018. The Department of State International Cyberspace Policy Strategy released in March 2016 described a whole-of-government approach to cyber deterrence, using all tools of national power. It stated that the United States would pursue deterrence by denial and deterrence by “cost imposition” (punishment), using diplomatic tools, law enforcement tools, economic tools, military capabilities, and intelligence capabilities.^[37] In May 2018, the State Department released “Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats,” and it defined a desired end state for U.S. cyber deterrence strategy. This end state would see an “absence of cyber-attacks that constitute a use of force against the United States...and allies” and a “significant, long-lasting reduction in destructive, disruptive, or otherwise malicious cyber activities directed against U.S. interests that fell below the threshold of the use of force.”^[38] This document also declared that the United States would use both deterrence by denial and deterrence by imposing consequences (punishment) against cyber adversaries.

These end states acknowledge that not all malicious cyber acts can be deterred, particularly lower consequence cyber-attacks, but they are not a clear parallel to the kinetic realm. As has been seen on the Korean Peninsula since 1953, not all lower-level kinetic attacks can be deterred, and the U.S.-ROK alliance focuses on deterring strategic attacks while defending against lower-level attacks. While it is yet unclear what type of cyber-attack would constitute a use of force, deterring all uses of force could be a difficult goal to achieve.

The DoD released its Cyber Strategy in 2018, with “defend forward” as a key tenet. Defined as disrupting or halting malicious cyber activity at its source, a strategy based on defending

forward makes alliances vital, and the U.S.-ROK alliance is on the front line against North Korean cyber threats. Regarding deterrence, this document said the Defense Department would “use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten US national interests, our allies...prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners...Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response.”^[39] This is similar to the State Department’s statements on deterrence but does add an extra priority on deterring cyber-attacks that would threaten DoD information security.

South Korea’s Ministry of National Defense publishes a Defense White Paper every two years, and cybersecurity has received increasing attention this decade in the white papers. However, the white papers have not clearly discussed cyber deterrence, and have instead focused on defense, organizational policy, human resources, technology acquisition, and international cooperation. Previously quoted in this paper was the 2016 Defense White Paper’s statement on guarding against North Korean cyber-attacks on critical infrastructure and military networks. The 2018 Defense White Paper acknowledged that North Korea continues to develop its cyber capability and personnel but refrained from specifically calling North Korea a cyber threat.^[40]

In April 2019, South Korea’s Blue House published the country’s National Cybersecurity Strategy, which mentioned deterrence but did not specify any particular malicious cyber actors. One of the three goals of the strategy is to respond to cyber-attacks, including strengthening “security capabilities to deter cyber threats.”^[41] To ensure cyber-attack deterrence, the strategy listed taking the following measures:

- 1) actively respond to all cyber-attacks that infringe upon national security and national interests by concentrating national capabilities,
- 2) strengthen preventive capacity by building a system that efficiently collects, manages, and eliminates vulnerabilities in cyberspace, and
- 3) acquire practical capabilities to analyze causes of cyber attacks and identify the culprits.^[42]

The cyber deterrence thinking described here sounds more like deterrence by denial, and unlike recent US cybersecurity strategy documents, there is no explicit mention of using all tools of national power to establish a deterrence by punishment posture. Similar to South Korea’s Defense White Papers, protection of critical infrastructure and national networks receives top priority in the National Cybersecurity Strategy.

V. APPLYING CYBER DETERRENCE METHODS IN THE U.S.-ROK ALLIANCE

The cyber policy documents released over the last few years by the US and South Korean governments show that they are interested in establishing a cyber deterrence posture, and the U.S.-ROK alliance recognizes the need to deepen their cyber cooperation. Washington and

Seoul also seem to generally agree that deterring cyber-attacks on critical infrastructure and military networks are top priorities, but the allies may have some differences on what methods to use to enforce a cyber deterrence posture. This section will consider the four deterrence methods introduced in section 2 (punishment, denial, entanglement, and norms) and how those methods could be applied to deterring strategic-level North Korean cyber-attacks by the U.S.-ROK alliance, such as on critical infrastructure or military networks or as a force enabler for larger kinetic attacks.

The first method is deterrence by punishment, which US government agencies also have termed deterrence by cost or consequence imposition. This subtle semantic difference may be useful in thinking of all the ways to punish an adversary and get past the association with kinetic attacks, particularly nuclear attacks. All the tools of national power, including diplomatic, information, and economic tools, could be used to punish North Korea. Punishment methods also should include both in-domain punishments and cross-domain (non-cyber domain) punishments.

Table 1. Cyber deterrence by punishment

Options	Pros and Cons
<p>In-domain</p> <ul style="list-style-type: none"> - Disruption of civilian or military networks - Sabotage of digital military assets - Information operations aimed at sowing social unrest <p>Cross-domain</p> <ul style="list-style-type: none"> - Legal action against cyber corps operating outside of DPRK - Diplomatic sanctions - Targeted economic sanctions - Kinetic strikes on cyber corps or civilian/military infrastructure 	<p>Pros</p> <ul style="list-style-type: none"> - Places cyber deterrence well within overall U.S.-ROK deterrence posture - Strong deterrent signal against high-impact cyber attacks <p>Cons</p> <ul style="list-style-type: none"> - Timely, convincing attribution - Appropriate targets and proportionality^[43] - Credibility of threat can be doubted

Table 1 summarizes punishment options and the pros and cons of such a posture. The biggest challenge to this method is finding punishments that the United States and South Korea would be able and willing to enforce, that produce a deterrent effect on North Korea, and can be credibly signaled to North Korea. If the allies cannot find punishments that meet those conditions, then they may be forced to pursue one of the other methods.

Table 2. Cyber deterrence by denial

Options	Pros and Cons
<ul style="list-style-type: none"> - Increase resiliency and ability to recover - Increase redundancy in critical networks and systems - Improve supply chain and personnel security 	<p>Pros</p> <ul style="list-style-type: none"> - Increases time and effort for DPRK to achieve goal^[40] - Increases failure rate for DPRK - Best practices applicable to cyber defense in other sectors <p>Cons</p> <ul style="list-style-type: none"> - Cannot prevent all attacks - Must stay ahead of adversary's techniques

Table 2 summarizes options and pros and cons for deterrence by denial. Given the challenges with punishments in the cyber domain, this is probably the default cyber deterrence posture. It mostly requires bolstering cyber defenses and credibly signaling to North Korea that cyber attacks will not achieve their desired goal because of those defenses. A significant challenge would be trying to maintain such a posture in the face of a determined, persistent adversary like North Korea, who likely will defeat defenses at some point.^[45]

Tables 3 and 4 summarize options and pros and cons for entanglements and norms, the two other cyber deterrence methods introduced by Nye. These two methods would likely work best if combined with either punishment or denial. Lacking a deterrence by punishment or denial posture, deterrence failure with these two methods would leave the U.S.-ROK alliance vulnerable with insufficient defenses or counterattack capability. However, using deterrence by entanglement or norms could open new ways to use non-military tools of power to enforce cyber deterrence, such as by tying the current diplomatic processes on the Korean Peninsula or external economic engagement projects with malicious North Korean cyber behavior. But such options also would require convincing North Korean leadership that these things are in their interest or agreeing to uphold norms, and North Korean history does not suggest that this would be easy or likely to happen.

Table 3. Cyber deterrence by entanglement

Options	Pros and Cons
<ul style="list-style-type: none"> - Increase DPRK economic and social interdependence on the Internet - Tie current U.S.-DPRK and ROK-DPRK diplomatic processes to malicious DPRK cyber behavior 	<p>Pros</p> <ul style="list-style-type: none"> - Can lead to self-deterrence by DPRK and preference for stability - Avoids escalation ladders and cyber arms races <p>Cons</p> <ul style="list-style-type: none"> - DPRK has low degree of interdependence with international economic system - DPRK leadership may resist further interdependence - DPRK leadership views cyber as critical asymmetric tool and integral to war planning

Table 4. Cyber deterrence by norms

Options	Pros and Cons
<ul style="list-style-type: none"> - Engage DPRK on agreeing to norms in cyberspace - No targeting of civilians in peacetime - Apply laws of armed conflict in cyberspace - Propose cyber confidence building measures to work to agreement on norms^[46] 	<p>Pros</p> <ul style="list-style-type: none"> - Similar to entanglements <p>Cons</p> <ul style="list-style-type: none"> - Attribution is necessary^[47] - DPRK has not adhered to many international norms

VI. CONCLUSION AND RECOMMENDATIONS

Scholars and practitioners are still in early stages of applying deterrence theory to the cyber domain, but it is critical that the US and South Korea more deliberately and explicitly formulate a cyber deterrence posture for their alliance. The existing deterrence posture in the U.S.-ROK alliance is built from the US extended deterrence guarantee, which is backed by US nuclear weapons. Credibility of the extended deterrence guarantee is further bolstered by the US military presence in South Korea. This application of nuclear deterrence theory based on punishment may not directly apply to cyberspace, but broader deterrence theory can be applicable, using other deterrence methods, such as denial, entanglement, and norms.

Yet, like nuclear deterrence, any cyber deterrence strategy must be credible and effectively signaled to be successful. The U.S.-ROK alliance should move beyond stated commitments to increase cyber cooperation to integrating cyber deterrence into the alliance's overall deterrence posture. While integrating cyber deterrence into the U.S.-ROK deterrence posture, the allies also should recognize that cyber deterrence methods contribute to overall cyber strategy and should not be expected to deter all cyber-attacks. Just as cyber deterrence is a component of overall deterrence strategy, cyber deterrence is one component of an overall allied cybersecurity strategy.

With these thoughts in mind, this paper concludes with the following recommendations for cyber deterrence in the U.S.-ROK alliance.

◆ **The U.S.-ROK alliance should formulate a joint cyber deterrence strategy.**

The strategy should be part of overall alliance deterrence strategy. The strategy could be integrated into the Tailored Deterrence Strategy, considering the Tailored Deterrence Strategy addresses North Korea's strategic and asymmetric capabilities. The cyber deterrence strategy must first define what is to be deterred and what methods will be used to deter, and it should clarify roles for the US and South Korea. While deterring cyber-attacks that produce strategic effects should be the focus, employing persistent engagement to address lower level attacks could reduce the scope, scale, and frequency of such attacks. Finally, the strategy should address an issue not explored in this paper, which is pursuing partnerships in the region, namely China. Beijing's relationship with Pyongyang and the presence of North Korean cyber agents in China mean the U.S.-ROK alliance should seek ways to engage China on North Korea's cyber activities.^[48]

◆ **Build on existing cooperative mechanisms to form a combined cybersecurity unit under the Combined Forces Command.**

The US and South Korean militaries have a Cyber Cooperation Working Group, and DoD established a cyber operations-integrated planning element within U.S. Forces Korea last year.^[49] A combined cybersecurity unit would strengthen these efforts and signal to North Korea that the alliance is serious about deterring cyber threats. A combined unit also could make it easier to integrate efforts, share intelligence and practices, and dynamically deter, defend, and respond to North Korean cyber-attacks.

- ◆ **Improve understanding of North Korean cyber strategy.** A cyber deterrence strategy or combined unit will only succeed if the allies better understand the adversary. What are North Korea’s tactical, operational, and strategic goals in the cyber domain, and what cyber capabilities could they use to achieve these objectives? Why has there not been a North Korean cyber-attack that produced strategic effects yet? Can North Korean cyber behavior be predicted and preempted, and is the cyber activity a precursor of kinetic or other asymmetric attacks?^[50] How can North Korea be engaged on cyber norms and interdependence? Better understanding these types of questions is necessary for tailoring a cyber deterrence strategy against North Korea, and the U.S.-ROK alliance needs to work together and with external analysts to better understand a hard intelligence target like North Korea.
- ◆ **For South Korea, leverage the U.S.-ROK alliance as an asymmetric advantage.** South Korea has economic and technological advantages over North Korea, but the U.S.-ROK alliance is Seoul’s “core asymmetric factor.”^[51] The United States has successfully provided extended deterrence against strategic threats to South Korea for over 60 years, and it would be prudent for Seoul to apply this advantage now to the cyber domain. In particular, the US can improve options for deterrence by punishment, while South Korea focuses on denial and entanglement. For example, Washington has more power to employ economic sanctions and may be more willing and able to use powerful cyber tools against North Korea. South Korea can continue to improve its domestic cyber defenses and resiliency, which contributes to deterrence by denial. Relying on the US for punishment also could leave Seoul more space to continue diplomatic and economic engagement, with a goal of deterrence by entanglement and norms. However, South Korea should not become overly reliant on Washington or stretch the US extended deterrence guarantee too far.
- ◆ **For the United States, embrace South Korea as a partner in defend forward.** Malicious North Korean cyber activity is a threat to the US, but South Korea is the primary target of North Korean cyber-attacks. Working with the South Korean military, civilian government agencies, and private industry will improve US understanding of North Korean cyber capabilities, intentions, and operations. Deterring cyber-attacks on a critical ally is clearly in US national interests, but a partnership with South Korea will also help prevent North Korean cyber-attacks from reaching US targets. ♥

DISCLAIMER

This paper may not be cited or redistributed without the permission of the author. Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other U.S. Government agency.

Author Bio

Dr. James E. Platte

Dr. James E. Platte is an Assistant Professor with the U.S. Air Force Center for Strategic Deterrence Studies (CSDS). His teaching and research focus on nuclear deterrence and counterproliferation, with a regional focus on East Asia. Prior to joining CSDS in 2017, Dr. Platte was an intelligence research specialist with the U.S. Department of Energy, and he also has worked on nuclear counterproliferation with the Defense Intelligence Agency and the National Nuclear Security Administration. He received his PhD in International Relations from The Fletcher School of Law and Diplomacy at Tufts University and has held research fellowships with the National Bureau of Asian Research, East-West Center, Pacific Forum, the Council on Foreign Relations, and the Harvard Kennedy School.

NOTES

1. "U.S. Relations With the Republic of Korea," U.S. Department of State, 17 July 2018, <https://www.state.gov/u-s-relations-with-the-republic-of-korea/>.
2. "Joint communique of 50th U.S.-ROK Security Consultative Meeting," United States Forces Korea, 31 October 2018, <http://www.usfk.mil/Media/News/Article/1679753/joint-communique-of-50th-us-rok-security-consultative-meeting/>.
3. Jeffrey Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (April 2010), 1-2.
4. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17), 46.
5. Aaron F. Brantly, "The Cyber Deterrence Problem," Proceedings of the 10th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence, 2018, 32.
6. Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004), 10-11.
7. Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton, NJ: Princeton University Press, 1961.
8. Knopf, "The Fourth Wave in Deterrence Research," 10.
9. Nye, "Deterrence and Dissuasion in Cyberspace," 45.
10. Brantly, "The Cyber Deterrence Problem," 33-34.
11. Nye, "Deterrence and Dissuasion in Cyberspace," 53.
12. Nye, "Deterrence and Dissuasion in Cyberspace," 58.
13. Nye, "Deterrence and Dissuasion in Cyberspace," 58-61.
14. Nye, "Deterrence and Dissuasion in Cyberspace," 60.
15. "Summary of Department of Defense Cyber Strategy," U.S. Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, 1.
16. Republic of Korea Ministry of National Defense, *2016 Defense White Paper*, Seoul: Ministry of National Defense, 2017, 77-79.
17. Donghui Park, "Cybersecurity Spotlight: South Korea," University of Washington Henry M. Jackson School of International Studies, January 12, 2016, <https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/>.
18. Brantly, "The Cyber Deterrence Problem," 34.
19. "Mutual Defense Treaty Between the United States and the Republic of Korea," Yale Law School Lillian Goldman Law Library, 1 October 1953, https://avalon.law.yale.edu/20th_century/kor001.asp.
20. "Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting," U.S. Department of Defense, October 28, 2017, <https://dod.defense.gov/Portals/1/Documents/pubs/20171028-Joint-Communique-OSD-MND-October-17-Final-version.pdf>.
21. "Joint communique of 50th U.S.-ROK Security Consultative Meeting."
22. "Joint Communique of the 45th ROK-U.S. Security Consultative Meeting," U.S. Department of Defense, October 2, 2013, https://dod.defense.gov/Portals/1/Documents/pubs/Joint%20Communique_%2045th%20ROK-U.S.%20Security%20Consultative%20Meeting.pdf.
23. "Joint Press Conference with Secretary Hagel and Minister Kim Kwan-jin in the Republic of Korea," U.S. Department of Defense, October 2, 2013, <https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5316>.
24. "Nuclear Posture Review," U.S. Department of Defense, 2018, <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>, 21.
25. Young-joon Lee, Hyuk-jin Kwon, Jae-il Lee, and Dong-kyoo Shin, "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," *The Korean Journal of Defense Analysis* 30, no. 3 (September 2018), 441.
26. Christine Kim, "North Korea hackers stole South Korea-U.S. military plans to wipe out North Korea leadership: lawmaker," Reuters, 10 October 2017, <https://www.reuters.com/article/us-northkorea-cybercrime-southkorea/north-korea-hackers-stole-south-korea-u-s-military-plans-to-wipe-out-north-korea-leadership-lawmaker-idU.S.KBN1CF-1WT>.
27. Lee et al., "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," 438.
28. Duk-Ki Kim, "The Republic of Korea's Counter-asymmetric Strategy," *Naval War College Review* 65, no. 1 (Winter 2012), 4.
29. ROK MND, *2016 Defense White Paper*, 78.

NOTES

30. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," U.S. Cyber Command, April 2018, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>, 6.
31. Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *The Journal of Strategic Studies* 40, no. 1-2 (2017), 102.
32. Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," 106-107.
33. Donghui Park, "Cybersecurity Strategy Advice for the Trump Administration: U.S.-South Korea Relations," University of Washington Henry M. Jackson School of International Studies, February 7, 2017, <https://jsis.washington.edu/news/cybersecurity-strategy-advice-trump-administration-us-south-korea-relations/>.
34. "Joint Fact Sheet: The United States-Republic of Korea Alliance: Shared Values, New Frontiers," The White House, October 16, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new>.
35. "Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting."
36. "Joint communique of 50th U.S.-ROK Security Consultative Meeting."
37. "Department of State International Cyberspace Policy Strategy," U.S. Department of State, March 2016, <https://2009-2017.state.gov/documents/organization/255732.pdf>, 20-23.
38. "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," U.S. Department of State, May 31, 2018, <https://www.state.gov/recommendations-to-the-president-on-deterring-adversaries-and-better-protecting-the-american-people-from-cyber-threats/>.
39. "Summary of Department of Defense Cyber Strategy," 4-5.
40. "2018 년 국방백서 (2018 Defense White Paper)," Republic of Korea Ministry of National Defense, December 2018, http://www.mnd.go.kr/user/mnd/upload/pblict/PBLICTNEBOOK_201901160236460390.pdf, 18-22.
41. "National Cybersecurity Strategy," Cheong Wa Dae National Security Office, April 2019, https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf.
42. "National Cybersecurity Strategy."
43. Brantly, "The Cyber Deterrence Problem," 45.
44. Nye, "Deterrence and Dissuasion in Cyberspace," 56.
45. Nye, "Deterrence and Dissuasion in Cyberspace," 57.
46. Nye, "Deterrence and Dissuasion in Cyberspace," 61.
47. Nye, "Deterrence and Dissuasion in Cyberspace," 60.
48. Park, "Cybersecurity Strategy Advice for the Trump Administration: U.S.-South Korea Relations."
49. Mark Pomerleau, "Why DoD is starting a new cyber cell on the Korean Peninsula," *Fifth Domain*, 20 April 2018, <https://www.fifthdomain.com/dod/cybercom/2018/04/20/why-dod-is-starting-a-new-cyber-cell-on-the-korean-peninsula/>.
50. Lee et al., "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," 451.
51. Kim, "The Republic of Korea's Counter-asymmetric Strategy," 17.

Operational Decision-Making for Cyber Operations: In Search of a Model

Dr. Max Smeets | JD Work

ABSTRACT

The decision-making behind cyber operations is complex. Dynamics around issues such as cyber arsenal management, target assessment, and the timing of dropping a destructive payload are still ill-understood. Yet, limited published research has thus far explored formal theoretic constructs for better understanding decision-making in cyber operations. Multiple models help to understand and explain the courses of action through which state cyber missions are executed, including conduct or restraint of cyber effects operations against target systems and networks. This paper evaluates four models - surprise model, duelist model, mating-choice model, and the Black-Scholes model. Each model offers specific advantages and suffers characteristic drawbacks. While these models differ in application and complexity, each may provide insights into how the unique nature of cyber operations impacts the decision dynamics of cyber conflict.

Keywords: Cyber operations, timing, decision-making, Black-Scholes, vulnerability equities, arsenal management

I. INTRODUCTION

Conceptualization of operational art and logistics factors in cyber operations remains immature in published literature.^[1] However, these factors are the *sine qua non* of successfully executing strategic intent, sustaining campaigns over time, and managing resource investment in what are ever costlier offensive cyber capabilities in an environment of spiraling complexity. Despite this, the behavior of designers, operators, and decision-makers responsible for the conduct of national cyber missions is largely discussed without a theoretic construct that identifies the choices, tradeoffs, and associated determinants that influence the courses of action that arise during cyber conflict.

At the heart of the contemporary instantiation of much of the problem space is understanding cyber operations' distinct features. Indeed, there has been much writing on how

cyber operations have several features that differentiate them from other warfighting domains. According to a report from the *National Academy of Sciences*, cyber operations come “with high degrees of anonymity and with plausible deniability; [...] more uncertain in the outcomes they produce; [...] [and] involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of seconds to years.”^[2] Cyber operations are also transitory in nature: they are strongly time dependent in terms of their potential to cause harm to targeted systems.^[3] Finally, and perhaps most important, there are close similarities between cyber effects operations and espionage operations, or what in intelligence jargon is called Computer Network Exploitation (CNE) and Computer Network Attack (CNA).^[4] Former NSA and CIA director Michael Hayden writes:

Reconnaissance should come first in the cyber domain too. How else would you know what to hit, how, when—without collateral damage? But here’s the difference. In the cyber domain the reconnaissance is usually a more difficult task than the follow-on operation. It is tougher to penetrate a network and live on it undetected while extracting large volumes of data from it than it is to, digitally speaking, kick in the front door and fry a circuit or two. [...] Let me go further. An attack on a network to degrade it or destroy information in it is generally a lesser included case of the technology and operational art needed to spy on that same network.^[5]

The purpose of this paper is to help systematize our thinking on how these attributes of cyber operations affect decision making and conflict dynamics. We do this through assessing the potential value of formal modeling—drawing on different fields of research—to cyber conflict dynamics. More specifically, *to what degree can we model how the nature of cyber operations impacts decision-dynamics of cyber conflict?*

The importance of improved systematic thinking in this area has been raised as US government posture has changed over the past several years, moving explicitly towards a vision of cyber capabilities in ongoing employment, rather than as a “fleet in being.”^[6] Under the concept of persistent engagement, cyber operations will be conducted to demonstrate resolve, counter ongoing intrusion and attack campaigns that directly target sources of national power, and impose friction and cost on the hostile actors orchestrating these malicious activities.^[7] Pursuit of this strategic vision requires understanding both of how scarce and often-ephemeral advantage within the domain may best be leveraged for operational purposes, but also how adversary operators, planners and decisionmakers may interpret and respond to actions conducted in the course of options generation and capabilities employment.

Formal modeling and policy have influenced each other since the publication of Neumann and Morgenstern’s *The Theory of Games and Economic Behaviour*.^[8] While the interaction between the two fields has often been highly constructive, various unsystematic and confusing applications of game theory on policy issues exist.^[9] A common misunderstanding of the power of game theory is that it is treated as a descriptive rather than analytical tool. Instead, as

Duncan Snidal indicates, “[t]he real power of game theory, for both empirical and theoretical purposes, emerges when it is used to generate new findings and understandings rather than to reconstruct individual situations.”^[10] Snidal adds that “while the simplicity of game models leads to a clarity that illuminates social phenomena, the deductive apparatus of game theory allows us to infer new understandings about international politics.”^[11]

Furthermore, as an analytical tool, many are concerned about whether the lessons learned from formal analysis are mere spurious experimental results.^[12] Yet, as Thomas Schelling writes:

What can one learn [in games]. [...] Is not each game, especially ones that involve much human judgment and imagination and risk taking, a unique story that may never be repeated? [...] The answer is that games are not different from real experience. Anyone who goes through a Bay of Pigs, a Yom Kippur surprise attack, or a battle over the Falklands has had an enormous learning experience. For some it can amount almost to a rebirth. Each such crisis [however] is unique. Few people ever participate in enough of them to compare them or to get a sense of relative proportions. Whether one experienced the event personally or studied it as historian, one must beware of generalizing. The corresponding danger in games is probably no greater than in real experience possible less so because games can be replicated and varied experimentally.^[13]

Given the complexity of cyber operations, and the constantly changing character of the domain’s technical and tactical features, that a single “unified” theory of planning and decision making may serve to explain or estimate behavior by the varied actors, diverse capabilities sets, and highly heterogenous organizational structures by which task requirements are manned, trained, equipped, and executed. Within this limitation, however, it is expected that some models may have analytic if not predictive value as a lens to explore aspects of the wider problem space. The body of this paper assesses and compares four families of formal and game-theoretic models in their ability to infer new insights regarding the way the nature of cyber operations affects decision dynamics on (cyber) conflict. The next section briefly reviews an existing formal model applied to cyber conflict, that is Robert Axelrod’s surprise model, the only published study in the field to date. Section III, in turn, provides a different model on the timing of cyber conflict, the ‘Duelist model’, which also takes other actors into consideration. The third model, described in Section IV, comes from the field of biology: we show it has a fruitful application for attackers to decide when to drop a destructive payload or continue intelligence gathering. Finally, borrowing from Finance, we discuss the Black-Scholes model in Section V. The model provides a superior understanding of how to model arsenal dynamics for cyber commands and organizations.

The results are summarized in Table 1. Overall, we find that the field of cyber conflict—both scholars and practitioners—can draw significant insights from other disciplines to better capture the dynamics of cyber conflict. We have not yet fully tapped into this potential, but hopefully this paper has provided an initial avenue to do so.

Table 1. Application of Game Theoretic Models to Cyber Conflict

	I	II	III	IV
Models	Surprise	Duelist	Search	Black-Scholes
Field of Origin	Politics / Economics	International Relations	Biology	Finance
Conventional Application	When should a resource be exploited for surprise?	When two duelists approach each other, when should they shoot?	When should an individual stop searching for a mate?	How should I price an option with a potential expiration date?
Cyber Conflict Application, General	Timing of cyber conflict	Timing of cyber conflict	Transition from cyber espionage to destructive attack	Arsenal management
Cyber Conflict Application, specific	When to use a zero day exploit?	i. When to hit a target before a rival actor will hit the same target? ii. When to attack a rival before the rival attacks me?	When should an individual stop searching for a mate?	How to price an option with a potential expiration date?
Complexity	Simple	Simple – Moderately Complex	Moderately Complex	Highly Complex
Utility	<ul style="list-style-type: none"> - Using both concepts of ‘stealth and ‘persistence’ allows for better discussion of cyber operations Time dynamics. - Only useful if there is a clear overview of what determines an operations transitory nature. - Current application is highly problematic in terms of case study analysis. 	<ul style="list-style-type: none"> - The model’s primary weakness lies in the unlikelihood that all three basic assumptions hold. - But the model’s strength lies in its wide range of potentially applicability, if the three basic assumptions hold. 	<ul style="list-style-type: none"> - The model’s assumptions apply well to cyber conflict - Relatively simple application. - It cannot deal with non-linear processes. 	<ul style="list-style-type: none"> - The model provides a compelling way to capture the patching dynamic of software vulnerabilities. - The assumptions made are not easy to translate to cyber conflict. - The model is not only complex to develop, but will also be difficult to use to justify decision making.

Before turning to the discussion of the models, three caveats are provided. First, the models discussed here have been ordered from least to most complex, however, that increased complexity does not make the model necessarily more useful or accurate. Second, though game theory is referred to as the “mathematical study of strategic interaction,”^[14] the discussion here omits the quantitative elements here to the extent possible to focus on the underlying logic behind each model, in order to examine the transferability of this logic to the cyber domain. Third, there are two assumptions underlying all four models: i) states are the most important actors, and ii) states are rational.^[15] The rationality assumption implies that states are choosing the best option available to them, from a set of possible options or strategies.

II. MODEL I: RATIONAL TIMING OF CYBER SURPRISE

In 1979, Robert Axelrod published a paper, “The Rational Timing of Surprise”.^[16] The paper aimed to explore when a resource for surprise should be exploited. The article discusses several situations for which the model is relevant: using information from code breaking or spying, using a new weapon, or giving false information to a double agent. Despite the differences in cases, Axelrod argues that all of them present the same structural problem in determining whether to wait or immediately exploit the resource.

Axelrod develops a model with four parameters:

- i) The stakes vary over time; and the greater the stakes, the greater the gains from exploiting a resource.
- ii) There are costs to maintaining a resource, which does not necessarily have to be material costs.
- iii) Exploitation risks exposure.
- iv) Value is discounted over time—the assumption is that if the payoff were the same for exploiting a resource today or waiting until a future opportunity, the choice would be made to exploit it today.

In a later paper, Axelrod and Iliev applied this framework to cyber conflict.^[17] The article explicitly states that the model can deal with only one aspect of the problem, “the timing of a cyber conflict, either in the form of espionage or disruption.”^[18] As the authors state, “[t]he paper takes the point of view of an actor who has a resource to exploit a vulnerability in a target’s computer system, and a choice of just when to use that resource.”^[19]

The main conclusions of their model are straightforward. First, if a cyber resource is likely still useable in the future if not used today, an actor is less likely to use it today. Second, an actor is also less likely to use a cyber resource when there is a low probability of being able to use it again, i.e. where there is a low chance of “resource survival”.^[20] Third, the authors find that an actor is more likely to hold their fire if there is the expectation that the stakes are high in a rare event happening in the future. Overall, as Axelrod and Iliev state, at “[t]he heart of [the] model is the trade-off between waiting until the states of the present situation are high enough to warrant the use of the resource, but not waiting so long that the vulnerability the resource exploits might be discovered and patched even if the resource is never used.”^[21]

The work of Iliev and Axelrod is commendable in that the model makes it possible to incorporate a more refined understanding of the transitory nature of resources used during cyber operations. Unlike most earlier studies, in this paper issue is not presented as a binary variable, i.e. the idea that a resource can only be used once (‘single-use’), but rather as a continuous variable. Also, the scholars estimate two parameters that determine whether the resource will be available in the next time period; ‘stealth’ and ‘persistence’. In their own words, “[t]he Stealth

of a resource is the probability that if you use it now, it will still be usable in the next time period. The Persistence of a resource is the probability that if you refrain from using it now, it will still be useable in the next time period.”^[22] This distinction is important as the use of resources during one operation significantly increases the chances of the discovery in the next period.

In addition, the paper usefully distinguishes between different resources in contrast to the primitive notion that all cyber resources are similarly transitory in nature. Integrating this more nuanced understanding into their formal model means the scholars reconcile the contrasting views of earlier works discussed above (although they may fail to deliberately recognize this integration). The degree to which the cyber domain incentivizes a use-it-or lose-it dynamic or a waiting-for-the-right-moment dynamic depends on the type of capability and whether the stakes remain constant.

Existing research demonstrates the relevance of the rational timing model, but further development is still needed. Additional case study examples are required to provide further empirical depth. Furthermore, the study of Axelrod and Iliev has a primitive understanding of the requirements of cyber operations. For example, it is unclear if the model applies only to the use of exploits or also implants.

III. MODEL II: DUELING IN CYBERSPACE

The application of game theory to analyze conflict situations blossomed during the Cold War. In light of the progressive development of nuclear weapons and delivery systems, numerous recommendations were made whether a first strike against the Soviet Union was rational.^[23] Considering this situation, most scholars provided a simplified model in which each of the two states involved in a conflict have two strategies: first and second strike.^[24]

The principle family of models that followed from this analysis (initiated by David Blackwell and other mathematicians in the reports of RAND corporation in 1948-52^[25]) are two-person games of timing in an uncertain environment. These models are often referred to as ‘duelist models’^[26] and are metaphorically seen as two duelists approach each other: the longer one of them waits to fire, the more likely it becomes that the other will fire first therefore striking first (the accuracy function increases with time). On the other hand, the closer the duelists get, the more likely it becomes that the first to fire will hit and disable the other (if a player fires too late, the opponent may hit his target earlier and the game may be terminated as the player has lost the opportunity to engage).

The basic features of this family of models are described by Radzik in a review paper entitled “Results and Problems in Games of Timing.” These features are each player has one bullet, which may be fired at any time; accuracy (i.e. the probability that the player hits) increases over time, and; the player who first hits the target is the winner and ends the game.^[27]

The duelist models could differ in several ways based on additional assumptions. First, the settlement of payoffs in this game can be arranged in two manners. The first pay-off structure produces a zero-sum game, the latter leads to a nonzero-sum game with various outcomes: The winner receives one ‘unit’ from his opponent, that is, each player wishes to maximize his expected return (this is in line with the classic duelist model). The winner receives one ‘unit’ from the umpire of the contest. That is, each player wishes to maximize his winning probability (this is more like a marksmanship contest). Second, there are two information patterns available to players: i) A player is informed of his opponent’s action time as soon as it takes place (this action is referred to as ‘noisy bullet’ or ‘noisy action’). ii) Neither player learns when or whether his opponent has acted (i.e. ‘silent bullet’ or ‘silent action’).^[28]

Third, there are different interpretations as to what ‘uncertain environment’ could entail. The following accuracy functions have previously been solved: i) When there is imperfect ability to perceive opponent;^[29] when duelist have uncertain knowledge about the existence of a bullet fitted to their guns;^[30] when the appearance of the object is random and whether or not the players are able to obtain the object is uncertain;^[31] when the bullets are only accessible at random times;^[32] when one player has one noisy bullet and one silent bullet and is forced to fire the former first, whereas the other player has only a silent bullet.^[33]

The value of this model would, like the previous model of Axelrod and Iliev, be in the timing of cyber conflict. However, the specific application of the model is slightly different: if I have a zero day exploit, and I know another actor has the same exploit, when should I use mine?^[34] In Axelrod and Iliev’s model, the use of your own exploit does not depend on whether the other actor has the same exploit. The chance of independent rediscovery of zero-day exploits is found to be relatively low. A study from RAND Corporation indicates that zero-day exploits have an average life expectancy of almost 7 years.^[35] Yet, about 25 percent of exploits will not survive for more than one and a half years, and another 25 percent will survive more than 9.5 years. Based on the data available, the RAND study was unable to provide any predictors on which *stockpiled* vulnerabilities are more or less likely discovered or disclosed.^[36] This data may be considered representative of Blue Force inventory, provided by contract acquisition to US and allied programs. One may infer similarities to other actors’ capabilities sets, although it may be presumed that zero-day exploits sourced from underground markets would be under greater collision pressure with commensurately shorter viable lifespans on the shelf.

Yet, considering the growth of the zero-day market, and the potential in which two or more actors may source capabilities acquired from the same entity due to opacity in gray and black-market transactions, the duelist model seems to describe a realistic scenario. These dynamics are further exacerbated by recurring features of vulnerability discovery and exploit development research, in which “interesting” operating system, application, and firmware/hardware targets attract similar development approaches across available attack surfaces, particularly where exploit engineers have relatively similar experiences and ongoing access to

earlier vulnerability disclosures from open source publication, private research communities, or the hacker “scene.”^[37] In this case, vulnerability collision may develop not as an unanticipated factor of common supply chains, but as an emergent feature of contemporaneous exploitation trends—the vulnerability zeitgeist, if you will.

The model’s primary weakness lies in the unlikelihood that all three basic assumptions will hold. The model’s strength lies in its wide range of potential applicability, if the three basic assumptions hold. The first assumption is that each player has only one bullet. Yet, it is to be expected that in most scenarios a state has more than one cyber option in inventory, or at least, could develop additional options within the actionable timeline of the conflict. The second assumption is that waiting pays off, as you have a higher chance of hitting the target. This model’s assumption goes against the assumption Iliev and Axelrod make: if you wait longer there is a higher chance that your exploit will be discovered; hence waiting does not pay off. Using this model in terms of a cyberattack, the value of gathering more info about your target and testing it outweighs the costs of potential discovery of the exploit. Whether or not this is the case is an empirical question and goes beyond the scope of this paper. Yet, one factor to consider is that the trade-off likely depends on how important the actor finds minimizing the undesired impact of offensive cyber operations. If the attacker cares a lot about collateral damage to other systems besides the intended target, the assumption of the duelist model is more likely to hold.^[38] The third assumption is that, if you do not strike, the other will strike against you—which also terminates the game.

During the early Cold War period, when the great powers did not yet have a second-strike capability, this assumption was highly applicable to reality. In relation to cyber conflict, however, could a preventive strike be beneficial? And what if this preventive strike could deny the other actor’s ability to ‘hit’ back? This proposition seems unlikely in the macro sense.^[39] It is highly unrealistic to expect that one actor could be able to conduct a preventive cyber operation, eliminating any possibility of the rival’s ability to retaliate through other cyber means. However, by targeting specific capabilities, employment mechanisms, or command and control infrastructure, that may have been enumerated through intelligence in advance of preventative action, this proposition may valid within specific operational windows for certain planning objectives. Indeed, this is one of the central concepts of cost imposition upon adversary actors through friction within the construct of persistent engagement, where the loss of certain capability options at a given moment of time forces investment in defending other surviving platforms, and regenerating new infrastructure, in order to accomplish espionage objectives and hold-at-risk operational preparation of the environment (OPE) posturing (prior to deployment at threshold of armed conflict.)

Beyond the application of these assumptions, however, this family of models offers a wide range of interesting logics to explore. First, following the above discussion on differences in pay-off structure and type of ‘bullet,’ the duelist model could serve different applications on the timing of cyber activity. These applications are summarized in table 2.^[40]

Table 2: Taxonomy of duelist model application to cyber conflict dynamics

	Noisy	Silent
Zero Sum	I. CNA against rival When should actor A conduct a destructive or disruptive cyberattack against actor B, before actor B attacks actor A?	II. CNE against rival When should actor A conduct a cyber espionage operations against actor B, when actor B is also interested in conducting the same type of operation against actor A?
Positive Sum	III. CNA against non-rival When should actor A conduct a destructive or disruptive cyberattack against a target of interest, when actor A knows that actor B might potentially attack this system too?	IV. CNE against non-rival When should actor A conduct a cyber espionage operations against a target of interest, when actor A knows that actor B might potentially attack this system too?

* This assumes that CNA activities are immediately discovered (i.e. noisy bullet) and espionage operations not (i.e. silent bullet).

** Rival actor means an actor which is also able to conduct a cyberattack against you. A non-rival concerns an actor you may want to conduct a cyberattack against, but is unable to attack you

Conventional application of the model could potentially be fruitfully applied to offensive cyber operations (i.e. imperfect perception of the opponent) in multiple ways. First, there are many situations in which the attacker has incomplete knowledge of the computer systems and networks of the target. Second, there may also be uncertainty about the potential undesired impact of a cyber operation (i.e. uncertain knowledge of the bullet). Third, as was stated above, CNA activities tend to follow after CNE activities. This means that a potential application of the ‘noisy and silent bullet’ is possible too, though the game set up must be reversed: first comes the silent bullet, and after that, the noisy bullet.

IV. MODEL III: SEARCH THEORY AND MATE CHOICE

The third potential model to consider is less conventional and comes from an application in the field of biology. Ever since Charles Darwin introduced his ideas on sexual selection in 1871, there has been an interest in understanding evolutionary change. The possibility of evolutionary change rests upon the notion that over time desired qualities in a species are more frequently passed on to each generation. In 1990, biologist Leslie Real wrote an influential evolutionary biology paper, “Search Theory and Mate Choice.”^[41] Real set up a model with the aim to resolve four questions:^[42] i) How do individuals find the best potential mates? ii) For how long should individuals search for mates for accepting a potential mate? iii) how are the critical values of acceptable mates determined? iv) What are the implications of increased mate competition, environmental uncertainty, variables survival, and/or mating costs for the decision-making process?^[43]

Real built her analysis upon the assumptions made by Janetos’ earlier model on what may constitute an optimal policy for mate choice.^[44] The following five assumptions underlie Janetos’ model(s): i) Individuals mate only once at any time, meaning that the model is implicitly restricted to monogamous or serially monogamous mating systems. ii) Mates are dispersed

in space such that they are encountered randomly with respect to fitness. iii) Only one of the sexes is discriminating. iv) The probability of a mate having a charitable fitness is based on a cumulative-probability density function (with a certain mean and standard deviation). The probability of an individual's mating depends only on its inherent, W , and the response of the actively searching mate.

Real argues that Janetos neglected a key feature of the problem, which led to significant biases in the model: the cost of searching and sampling.^[45] This radically changes the relative performance of the different strategies. In Janetos' model, with no search costs, a best-of- n is the best strategy: the searcher should sample all potential mates in the population before making a decision. In the case of Real's model, there is a growing cost for the mate to continue the search. As Real shows, this means that now a sequential-search model will always dominate.^[46] Also note that increased search costs reduce the threshold critical value for mate acceptability.

At first sight, it seems that the situation of evolutionary biology is very different compared to offensive cyber operations. However, the search model could have several fruitful applications for cyber conflict decision making. Whereas the search model in biology imagines an individual who must decide to accept or reject a mate on the basis of the sequence of encounters and a knowledge of the distribution of mates' qualities, in conducting cyber operations we can imagine an attacker who must decide to either deliver a destructive payload or continue intelligence gathering on the basis of the sequence of systems it has gained access to and the knowledge of the distribution of other system's importance.

The key point is that, if an attacker decides to only conduct espionage activities the chances of discovery are low. In cases where the attacker uses a zero-day exploit to access the system, it may be able to re-use this exploit for a prolonged period.^[47] Yet, if it decides to drop a destructive payload the chances of discovery are suddenly vastly higher. This leads to an important trade-off: when to move from espionage to disruptive or destructive activities (or from CNE to CNA)?^[48]

The search model provides an excellent framework to analyze this question. First, the key decision value in this respect is not 'mate quality' but the value an actor gains from dropping a destructive payload. Second, like searching for a mate, there are also costs in terms of continuing cyber espionage operations. There are the costs of the conducting the early phases of a cyber operation—reconnaissance, intrusion, privilege escalation, and lateral movement—to compromise a new system and / or network. There may also be costs to remaining stealthy in case an actor wants to maintain access to a certain system. In addition, potential other costs concern the potential patching of an exploit by the vendor or other change in the operating environment. Third, in the search model, the individual must consider what the expected fitness would be from sampling an additional 'passive mate'. In turn, an actor conducting a cyber operation must consider the expected value from intruding an additional computer system or network (i.e. what is the chance that there will be another system out there which is more valuable to intrude and drop a destructive payload?)

Table 3: Overview key parameters search model: Mate choice vs. cyber attacks

Variable	Mate Choice	Cyber Operation
w_{crit}	Decision variable: the minimally acceptable mate quality	Decision variable: the minimally acceptable strategic value gained of dropping a destructive payload
c	Cost of searching	Cost of continuing cyber espionage activities
$F(w)$	The expected fitness gain from sampling one additional passive mate	The expected value from intruding an additional computer system or network

* For a more comprehensive overview of the equation and variables see: Real, p. 384.

** The cumulative costs in the case of cyber-attacks could be negative, i.e. value from searching. For example, if the attacker gains knowledge of the system which is in and of itself valuable. For example, let us imagine an actor aims to attack an oil refinery. If the espionage activity itself provides valuable information regarding the process of refinery, which the actor can use, it can offset the costs of dropping a destructive payload.

A key weakness of the search model of Real is that it ignores mutual mate choice in which both sexes are choosy; there are only ‘passive mates’ in this environment. Although this assumption is problematic in her model, this assumption is more likely to hold for cyber-attacks; after all, no target generally wants to be attacked (honeypot and other deception systems excepted).

However, “choosiness” may be observed in real world action at differing points in more sophisticated offensive operations. Payload deployment choices may be constrained by temporal characteristics where the intended effect is not merely simple destructive execution (i.e. rm -rf like commands in simplified expression), but rather more complex degradation of functionality, particularly in ways that are less detectable or traceable. Such effects—including manipulation of system, application, sensor, and/or data integrity—are often highly sensitive to target configuration, workload factors, and other features. These may influence the “best match” option at varying points in time throughout the course of an operation or longer campaign. An easily considered example of such a case might be given based on business continuity processes, in which destructive or integrity-degrading effects offer variable impacts depending on time between back-up cycles. More sophisticated modeling may be required across heterogenous target sets, as may be encountered within an Integrated Air Defense System (IADS) network composed of equipment acquired across multiple generations and knit together with architectures of differing original design and retrofit modification. Likewise, there is much variability in destructive payload effects, and further effects beyond simple destruction, which may provide differing complexities for analysis under this model.

V. MODEL IV: CAPABILITIES OPTION “PRICING” AND THE BLACK-SCHOLES MODEL

The final model is from modern option pricing (i.e. a form of hedging) in finance.^[49] The notion of options is centuries old. In the 16th century, grain dealers in Amsterdam were said to use options. A century later, Joseph de la Vega provided the first heuristic method to price and deal with exposure. And more sophisticated techniques emerged in the 19th century as

the financial markets developed in London, Paris, and New York. Charles Castelli was the first to provide a theory of hedging in 1877.^[50] Bachalier followed with a theory of speculation in 1900.^[51] Modern option pricing was reborn in the 1950s. In 1955, Paul Samuelson famously published his work on Brownian Motion in the stock market. Black and Scholes in 1973 provide a new method to price options and corporate liabilities.^[52]

Following this work, the Black-Scholes equation is the main tool used to price options in today's market. Buying an option means buying the right to engage in a particular transaction, yet the buyer has no obligation to follow through on the transaction.^[53] There are three types of options: a European option may be exercised only at the expiration date of the option, an American option may be exercised at any point before the expiration date of the option, and a Bermudan option may be exercised only on pre-determined dates before the expiration date of the option, typically a month.

To price an option, one tries to find a way to value its 'dynamic hedge,' that is, mirror the option's payout using the underlying asset. When one initially creates a riskless delta hedge, it is only riskless at the instant it is created.^[53] Hence, it needs to be continuously rebalanced. This requires a 'dynamic' hedge. The Black-Scholes has (at least) five pricing inputs: i) spot price of underlying asset, ii) options strike price; iii) risk free rate, iv) volatility returns of the underlying asset, and v) time-to-expiry.

It rests on the following assumptions: i) presence of constant risk-free rate; ii) efficient market hypothesis holds; iii) securities are infinitely divisible (i.e. it is possible to buy any fraction of a stock); iv) no restrictions on short selling; v) no opportunity for arbitrage; vi) the price of the underlying follows a log-normal distribution; and vii) the return of the underlying follows a normal-distribution. These assumptions are subject to much criticism, and there are methods available to relax some of them, however the initial model shall suffice for this analytic purpose.

Conventional weapons' aging is generally modeled as a gradual (log-linear) deterioration. Yet, this typical type of function does not hold up for cyber operations. The malleability of cyberspace offers, in the words of Bruce Schneier, a unique "window of exposure" for cyber-attacks to be effective.^[54] The life-cycle of a vulnerability normally follows the following stages: vulnerability introduction, vulnerability discovery, creation of exploit for vulnerability, awareness vulnerability by the vendor, vulnerability is publicly reported, and release of the patch. The procedure of these stages is not a (log)linear process. Instead, the ability to use an exploit damage remains constant for a certain period of time, but rapidly declines the moment the vendor discovers the exploit, or a third party with visibility into the exploit informs the vendor.^[55] Indeed, the decay function of an exploit is characterized by 'random crashes.'

The Black-Scholes model might provide a way to model this dynamic of this life cycle. The use of an exploit is similar to an ‘American option’ (i.e. it can terminate at any time). The value of using an exploit could be modeled as a ‘Brownian motion’ with random crashes. These random crashes may be caused by cases when other actors have used the same exploit, or when the vendor becomes aware of the vulnerability without an actor having used it in the past. Such instances may result from independent vulnerability rediscovery, or from visibility derived from detection through defensive countermeasures or through counter-cyber operations against other similar capabilities deployed from equivalent resource inventories held by other actors. The model assumes that the capability price fluctuates with constant drift and volatility, which leads to a geometric Brownian motion model for the price path.

Exploit inventory value crashes may also result from vulnerability discovery occurring based on identification of similar exploit chain components in other uses, including both primitives as well as weaponized exploitation in the wild. This, too, may have an underlying “physics-like” modeling property based on the fundamental characteristics of formal mathematical proof of exploitability (or more likely unexploitability), in which multiple pathways may be found to reach the same “weird machine” state of unintended code behavior.^[56]

Overall, unlike the model of Iliev and Axelrod, or other more primitive models, when applied to cyber-attacks, this model does not assume that the loss of an exploit’s value is a linear or log linear function. Instead, if one incorporates a model with ‘random crashes’ it provides a much closer representation of reality. In that sense, setting up this type of model could help government institutions to obtain a better cost estimate of arsenal maintenance.^[57]

VI. CONCLUSION

This paper assesses to what degree (and which) formal models help to explain strategic choice and behavior in relation to cyber conflict. To this end, this paper discussed four models: one model already previously discussed by Axelrod and Iliev and three new models in relation to cyber conflict. All four models are potentially useful in explaining certain cyber conflict dynamics, although they have different strengths and weaknesses. It was never the aim of this paper to be comprehensive; there will be many deserving models and issues that are not covered or cited here. Instead, it is hoped that the models discussed here will serve as a useful doorway into a more structured understanding of cyber conflict dynamics.

Modeling the range of the future decision space under a variety of potential scenarios finds new relevance as offensive cyber operations (OCO) and counter-cyber operations (CCO) activities are considered beyond the episodic events which surface as major headlines from time to time, but instead are more deeply considered as the product of sustained organizational and individual efforts by military, intelligence, and proxy forces in pursuit of competitive objectives below the threshold of armed conflict, in preparation for future conflict, or seeking advantage in ongoing disputes that push gray zone thresholds.^[58] There is an underlying logic that dictates the course, pace, and evolution of such operations by rational actors with differing interests, balancing differing equities. To date, these logics have been understood only dimly through analogy to other warfighting domains, and through inherited conceptual frameworks. The argument has been made that offensive cyber capabilities are perhaps the first military innovation to emerge directly from the intelligence community.^[59] If one accepts this well-supported hypothesis, it is understandable then that cyber operations to date have followed the logic of intelligence operations.^[60]

However, as emerging capabilities are coupled ever more tightly with conventional national security strategies, and across military globally integrated operations concepts, extant logics may well be changing. At the very least, new players and new priorities are likely to alter considerations of equities balancing, and perceptions of constraints, restraint or the lack thereof will likely differ as new audiences consider what were previously decisions taken in more rarified and classified environments. The different mechanisms for signaling, public disclosure, parliamentary oversight, as well as generating and sustaining the public support that accompany military operations may also play key roles in influencing decision-making.

Thus, much additional work is needed to capture the complexity, variability, and path-dependence of offensive decision-making in cyberspace. This work may also be further enriched by more detailed insight into adversary specific strategic cultures (to the extent that such cultures may or may not be observed to exist), organizational influences, and operational experiences. Likewise, much of the decision space in which such logic is exercised is heavily influenced by the intelligence picture available to leadership, and where lacunae exist due to collection gaps, analytic failures, or deliberate deception impacts, the potential for misperception creates as yet unexplored strategic and operational risks.^[61]

Beyond theoretic constructs, it is almost certain that the rapidly accelerating pace of current events shall see the employment of capabilities and response by other states, many times over across ongoing crisis flashpoints. It is expected that a robust body of case examples will result from these events, which may offer unique insights for future analysis and modeling. 🛡️

Author Bios

Dr. Max Smeets

Dr. Max Smeets is a senior researcher at the Center for Security Studies (CSS). He is also an Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford. Max was previously a postdoctoral fellow and lecturer at Stanford University CISAC and a College Lecturer at Keble College, University of Oxford. He has also held research and fellowship positions at New America, Columbia University SIPA, Sciences Po CERI, and NATO CCD COE. Before his academic career, Max worked in finance in London and Amsterdam. He received a BA in Economics, Politics and Statistics summa cum laude from University College Roosevelt, Utrecht University and an M.Phil (Brasenose College) and DPhil (St. John's College) in International Relations from the University of Oxford.

JD Work

JD Work serves as the Bren Chair for Cyber Conflict and Security at the Marine Corps University, leading efforts developing the theory, practice, and operational art of the cyber warfighting function, and to explore the wider role of the cyber instrument in national security strategy and the future defense competition, and stability problem space. Mr. Work has over two decades experience working in cyber intelligence and operations roles for the private sector and U.S. Government. He previously directed multiple international research programs to provide insight into the emerging strategic issues, economic consequences, and technology implications created by hostilities in the information environment, in order to support early warning, crisis management, and crisis prevention in and through cyberspace. Mr. Work also holds appointments with Columbia University School of International and Public Affairs, Saltzman Institute of War and Peace Studies, as well as the George Washington University Elliot School of International Affairs. He further serves as a senior advisor to the U.S. Cyberspace Solarium Commission.

NOTES

1. Application of game theory constructs to strategic and functional future cyber operational planning is known to have been conducted in nonpublic communities of interest associated with major national capabilities since at least 2008, building on related prior work examining the similar challenges regarding signals intelligence decision-making.
2. William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds.), "Excerpts from Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", National Research Council, (2009); S-1, Section 1.4 and 2.1.
3. Max Smeets, "On the Transitory Nature of Cyber Weapons," *Journal of Strategic Studies*, (2017)1:28
4. Matthew Monte, *Network Attacks and Exploitation*, (Wiley, 2015)
5. Hayden also writes: "I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones)." Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, New York, Penguin Random House, 2016, 137.
6. John B. Hattendorf. "The Idea of a 'Fleet in Being' in Historical Perspective." *Naval War College Review*, 67:1 (2014).
7. Paul M. Nakasone. "A Cyber Force for Persistent Operations. *Joint Force Quarterly*. 92: 1st Quarter 2019.; Michael P. Fischerkeller, Richard J. Harknett. "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," Institute for Defense Analyses, Alexandria, VA, May 2018; For review of strategy's potential impact also see: Max W.E. and Herbert Lin, "4 A Strategic Assessment of the U.S. Cyber Command Vision," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Herbert Lin and Amy Zegart (eds.) (Brookings Institution Press: 2018).
8. Neumann and Morgenstern's work is usually considered to be the first systematic and extensive formal analysis of social interaction. See: John von Neumann and Oskar Morgenstern, *Theory of Games and Economic Behaviour*, Princeton University Press: Princeton, 1944; Also see: Jacob Marschak, "Neumann's and Morgenstern's New Approach to Static Economics", *Journal of Political Economy* 54 (1946), 97–115.
9. This is hardly surprising as the subject matter of international relations is often seen as the study of the interactions themselves. See Lake, David H. and Powell, Robert (eds.), *Strategic Choice and International Relations*, Princeton University Press: Princeton, 1997.
10. Duncan Snidal, "The Game Theory of International Politics," *World Politics*, 38-1(1985), 25-57.
11. *Ibid*, 28.
12. Paul K. Davis, "Studying First-Strike Stability with Knowledge Based Models of Human Decision making," Washington DC., RAND, 1989.
13. Thomas C. Schelling, "The Role of War Games and Exercises," in Carter et. al. (Eds.), *Managing Nuclear Operations*, The Brookings Institution, Washington, D.C., 1987, 439-440.
14. Andrew Kydd, *International Relations Theory: The Game-Theoretic Approach*, Cambridge: Cambridge University Press: 2015.
15. While discussion of these models may be usefully extended in the context of nonstate actors, further work is required to explore these dynamics in other contexts.
16. Robert Axelrod, "The Rational Timing of Surprise," *World Politics*, 31:2, (1979), 228-246.
17. Robert Axelrod and Rumien Iliev, "Timing of cyber conflict," *PNAS*, 111:4 (2014), 1298–1303.
18. *Ibid*.
19. *Ibid*.
20. *Ibid*.
21. *Ibid*.
22. *Ibid*.
23. William Poundstone, *Prisoners' Dilemma*, Anchor Books: New York, NY, 1993, 141.
24. Alan D. Taylor, *Mathematics and Politics: Strategy, Voting, Power and Proof*, Springer Verlag: New York, 1995, 166.
25. David Blackwell, *The noisy duel, one bullet each, arbitrary accuracy*, The RAND Corporation: 1949; David Blackwell and A. Girshick, "A loud duel with equal accuracy where each duelist has only a probability of possessing a bullet", The RAND Corporation: 1949, David Blackwell and A. Girshick, *Theory of Games and Statistical Decisions*, John Wiley, New York: 1979; for an excellent review see: Tadeusz Radzik, "Results and Problems in Games of Timing, Statistics, Probability, and Game Theory," *IMS Lecture Notes Monograph Series*, 30, (1996).

NOTES

26. See Ken Binmore, *Fun and Games: A Text on Game Theory*, D. C. Heath and Co: Lexington, 1992; Melvin Dresher, *The Mathematics of Games of Strategy: Theory and Applications*, Dover Publications Inc.: New York, 1981.
27. Radzik, “Results and Problems in Games of Timing”.
28. Yoshinobu Teraoka, “Two-Person Game of Timing with Random Termination,” *Journal of Optimization Theory and Applications*, 40: 3 (1983).
29. Calvin W. Sweat, “A single shot noisy duel with detection uncertainty,” *Operation Research*, 19 (1971), 170-185.
30. Yoshinobu Teraoka, “Noisy Duel with Uncertain Existence of the Shot,” *International Journal of Game Theory*, 5 (1976), 239-249, 1976; Yoshinobu Teraoka, “Silent-Noisy Duel with Uncertain Existence of the Shot,” *Bulletin of Mathematical Statistics*, 18 (1981), 43-52.
31. Teraoka, “Two-Person Game of Timing with Random Termination.”
32. S. Styszyński, “A Silent-Silent Duel with Bullets Accessible at Random Moments,” *Politechniki Wrocławskiej, Instytut Matematyki, Research Report*, No. 40 (1979).
33. T. Kurisu, “On a Noisy - Silent versus Silent Duel with Equal Accuracy Functions,” *Journal of Optimization Theory and Applications*, 39 (1983), 215-235.
34. The model could potentially account for adding a *probability* that the other actor has the same exploit.
35. Lillian Ablon and Andy Bogart, “Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits,” RAND Corporation: 2017.
36. Ibid.
37. Discussion with vulnerability researchers under Chatham House rule, Marine Corps University, June 2019.
38. For a lengthier discussion on this point see: David Raymond, Greg Conti, Tom Cross, and Robert Fanelli, “A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons”. 2013 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.) 2013 © NATO CCD COE Publications, Tallinn https://ccdcocoe.org/uploads/2018/10/8_dlr2s6_raymond.pdf, <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=67E85114AA1D5C3942296FA224578088?doi=10.1.1.385.7204&rep=rep1&type=pdf>.
39. Also see: Max Smeets, “The Strategic Promise of Offensive Cyber Operations,” *Strategic Studies Quarterly*, Fall 2018, 90-113; Max Smeets and Herbert S. Lin, “Offensive Cyber Capabilities: To What Ends?” 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, T. Minárik, R. Jakschis, L. Lindström (Eds.) 2018, NATO CCD COE Publications, Tallinn.
40. For a discussion on similar trade-offs see: Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, University of Georgia Press, 2016, 79 – 89; Brantly, “Aesop’s Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace.” *Intelligence and National Security* 31, no. 5 (2015), 674-85, <https://doi.org/10.1080/02684527.2015.1077620>.
41. Leslie Real, “Search Theory and Mate Choice. I. Models of Single-Sex Discrimination”, *The American Naturalist*, 136-3(1990):376-405; also see: Leslie Real, “Search theory and mate choice: II. Mutual interaction, assortative mating, and equilibrium variation in male and female fitness,” *American Naturalist*, 138:(1991) 901–917; Russell Bonduriansky, “The evolution of male mate choice in insects: a synthesis of ideas and evidence,” *Biological Reviews*, 76-3(2001), 305-339.
42. This model does not explicitly deal with the behavior of rivals in a game theoretical sense, i.e., the strategy of other actors is not considered, merely a modeling term is added that considers the risk of waiting.
43. Ibid, 377.
44. Anthony C. Janetos, “Strategies of female choice: a theoretical analysis,” *Behavioral Ecology and Sociobiology*, 7 (1980), 107-112.
45. Real divides the costs of sampling into two forms. First, there are ‘direct costs’ which concerns aspects such as expenditures of time and energy through added search, directed aggression from other competing searchers, risk of predation, or death. Second, there are ‘indirect costs’ (or opportunity costs) which includes aspects such as loss of previously encountered mates due to death, emigration, or loss of mating status.
46. According to Leslie Real, “the problem is formally analogous to a variety of classic sequential-search models discussed in the literature of both economics and statistics. The problem, variously known as the secretary problem, marriage problem, and job-search problem, imagines an agent who must decide to accept or reject candidates based on the sequence of encounters and a knowledge of the distribution of candidate qualities.” Real, “Search Theory and Mate Choice.”

NOTES

47. However, the use of zero-day exploits is much less common than some would think. See: Rob Joyce, “Disrupting Nation State Hackers,” *USENIX Enigma 2016*, retrieved from: https://www.usenix.org/sites/default/files/conference/protected-files/engima2016_transcript_joyce_v2.pdf.
48. Also see: Max Smeets, “Organizational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks”, in Henry Roigas, Raik Jakschis, Lauri Lindstrom, and Tomáš Minarik (Eds), 9th International Conference on Cyber Conflict, Tallinn, NATO CCD COE Publications: 2017; Max Smeets, "Integrating offensive cyber capabilities: meaning, dilemmas, and assessment," *Defence Studies*, 18:4 (2018), 395-410.
49. In the market there are two ways to think about hedging; i) loss mitigation for an asset, and ii) the creation of a diskless portfolio. Option pricing uses the second of these definitions.
50. Charles Castelli, *The Theory of Options in Stocks and Shares*, London: F. C. Mathieson: 1877.
51. Bachelier, “The Theory of Speculation”, *Annales scientifiques de l’Ecole Normale Supérieure*, 3:17 (1900), 21-36 (Translated by May) retrieved from: <http://www.radio.goldseek.com/bachelier-thesis-theory-of-speculation-en.pdf>.
52. Fischer Black and Myron Scholes, “The pricing of options and corporate liabilities,” *The Journal of Political Economy*, 81:3 (1973), 637–654.
53. Jacob Abernethy, Rafael M. Frongillo, and Andre Wibisono, “Minimax Option Pricing Meets Black-Scholes in the Limit,” STOC’12, (May 19–22, 2012, New York, USA).
54. Bruce Schneier, “Crypto-Gram,”(2000), <http://www.schneier.com/crypto-gram/archives/2000/0915.html>.
55. Smeets, “A Matter of Time.”
56. For further exploration of the concepts of formal proof in exploitation, see the unique work of Thomas Dullien. "Weird machines, exploitability, and provable unexploitability." *IEEE Transactions on Emerging Topics in Computing*. December 2017. DOI: 10.1109/TETC.2017.2785299.
57. Again, note that the use of exploits is only one small part of the military cyber arsenal.
58. Also see: Florian Egloff, “Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates.” DPhil Thesis, University of Oxford, 2018.
59. Craig J. Wiener, *Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as A Major Military Innovation*, George Mason University, 2016.
60. Discussion under Chatham House rule at Strategic Competition in Cyberspace: Challenges and Implications. Center for Global Security Research. Lawrence Livermore National Laboratory, July 10-11, 2019.
61. The seminal work in this area of course remains Robert Jervis. *Perception and Misperception in International Politics*, Princeton, NJ: Princeton University Press, 1976; additional consideration specific within this new domain seems of value.

THE CYBER DEFENSE REVIEW

◆ TECHNICAL PAPERS ◆

Overview of 5G Security and Vulnerabilities

Shane Fonyi

ABSTRACT

The 5G wireless standard is currently in development and is slowly being rolled out to a few cities in the United States. There has been a concern for the security and overall architecture of the 5G standard from industry professionals and government officials. This paper will summarize the research done in the 5G security space and will provide an overview of the technologies used in 5G, the security built into 5G, and the vulnerabilities of 5G. The specific vulnerabilities researched are classified into the three pinnacle components of information security: confidentiality, integrity, and availability. The use of Internet of Things devices, medical collection devices, and massive device-to-device communications will also be discussed.

Keywords—5G, security, wireless, vulnerabilities, LTE

I. INTRODUCTION

Launched in 1979 in Tokyo, Japan, the first generation (1G) cellular wireless network was established. By 1983, the United States had launched its first 1G network and several other countries followed suit. Fast forward 30 years and 4G Long Term Evolution (LTE) had been deployed to select cities in Norway, Sweden, and Finland. According to Statista, the number of LTE subscriptions in 2019 are estimated to reach 4.7 billion.^[36] Throughout the evolution of wireless technology, the push to increase bandwidth and transmission speeds has been a catalyst for creating new wireless technology standards. Because of the increased abundance of transmission and technologies, wireless subscriptions are projected to rise. The large demand pushes industries to produce new technology that allows for greater innovation. Wireless speeds are tapering off worldwide as more devices come online and the allocated spectra in the respective countries are not able to keep up.^[38] With this latest push for faster speeds and better coverage comes the 5G wireless standard. The speed of different generations over the years are shown in Table 1.^[9]

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

The largest increase in bandwidth is from 4G LTE to 5G by looking at the table. Carriers are working to determine what 5G will look like as far as bandwidth goes. Verizon’s current tests give an idea of what the standard user might be able to expect from 5G.^[18] The 5G standard also includes a decrease in latency speed from 10 milliseconds to 1 millisecond.^[4] With this jump in speed and a lower round trip time, new uses for wireless networking will come. A common phrase in the information security community is that innovation moves at the speed of light and security is often left behind. The rise of Internet of Things (IoT) devices brings its own set of confidentiality and availability issues.

When developing a newer, faster technology, it is imperative to determine the changes that need to be made to allow for its successful integration. In the case of 5G, there are several changes to the current 4G infrastructure that will be discussed. It is important to note that while 5G is being deployed, much of the 4G infrastructure will remain in place. The following will be discussed throughout the paper: an overview of 5G; security for 5G features; and possible vulnerabilities identified within 5G. The paper concludes with an accounting of the information presented and a summary of the most important outcomes of 5G and the security built into the standard.

Table 1: Wireless Generation Speeds

Generation	Dates	Speed
1G	1980s	Voice Only
2G	1990s	SMS (text only messages) introduced
2.5G	2001-2003	Data below 100 kbps, Multimedia Messaging introduced
3G	2003-2010	1-2 megabits per second download
4G	2010	2-10 megabits per second download
4G LTE	2010	10-20 megabits per second download
5G	2019	200-634 megabits download*

*Table information retrieved from [9]. *From [18]*

2. OVERVIEW OF 5G

At this time, there are no concrete standards for 5G. There are currently several organizations working on finalizing these standards, including the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), and the Internet Engineering Task Force (IETF). The 3GPP is an organization that brings together seven telecommunication standard development bodies into one group.^[5] The IETF is an open international community of network professionals and researchers concerned with the future of internet architecture and operation.^[29] The ITU is an international specialized agency, that is a part of the United Nations, for information and telecommunication technologies.^[6] The ITU is the organization leading the charge for 5G standardization and has defined a timeline and project for submis-

sion and approval of 5G requirements called IMT-2020. The project was intended to determine and scope the requirements for the next generation networks in 2020 and the future. The 3GPP developed Release 15 for its 5G Phase 1 specifications and submitted to the ITU.^[4] The 3GPP is currently working on Release 16: 5G Phase 2 specifications and soon plans to submit to the ITU before the proposal submission window closes in mid-2019. A timeline produced by a 3GPP partner, ETSI, can be viewed in Fig. 1 that displays the current 5G standards proposed timeline from the ITU and how the 3GPP plans to incorporate their findings. Currently, the minimum requirements for technical performance related to IMT-2020 were set in ITU-R M.2410 and are the following ^[32]:

- ◆ Peak Data Rate: 20 gigabits per second (Gbps) Download/10 Gbps Upload
- ◆ Peak Spectral Efficiencies: 30 bits per second per Hertz Downlink/15 bits per second per Hertz Uplink
- ◆ User Latency: 4 ms for enhanced mobile broadband (eMBB), 1 ms for ultra-reliable low latency communications (URLCC)
- ◆ Control Plane Latency: 10-20 ms
- ◆ Maximum Aggregated Bandwidth: 100 MHz for frequency bands <1 GHz/1 GHz for bands > 6 GHz
- ◆ Mobility: Usable up to 500 KPH in rural eMBB

From the requirements, the focus of the next generation network is adding more devices and increasing speeds to the user equipment.^[32] User equipment (UE) includes home nodes, cell phones, computers, SCADA, ICS, IoT, etc. Any device that uses the cellular network to connect to the internet or to voice communications is UE in terms of wireless specifications. This broad range of devices makes it difficult to create specifications that allows the flexibility to incorporate the wide spectrum of devices. The proposal outlines an environment that will allow high speed communications from an end device to the internet and also very fast transactions between devices. This is where the URLCC comes into the fold to facilitate that type of quick communication. The timeline shown in Figure 1 shows that the expected finalization of the 5G standards will be early to mid 2020.^[19] There are still proposal submissions that will be reviewed for final concurrence on whether they will be added to the final specification. This means that 5G is not a complete specification whether or not it is being deployed as changes will likely need to be made in order to keep with the requirements.

2.1 Changes to 4G Architecture

While 5G deploys to large cities, it will be configured in a mode called 5G NR Non-Standalone (NSA). This mode will use the 5G NR (New Radio) standards and continue to utilize the existing 4G core infrastructure.^[40] The 5G NR standards include using spectrum sub-1 GHz, 1–6 GHz and above 6 GHz, including the mmWave frequencies above 24 GHz.^[25] The FCC has made

offering mmWave frequencies available a priority.[10] The implementation of NSA is highly dependent on the carrier. From an interview with a 5G research group for major network provider in the US, their company plans to provide broadband internet to households and businesses using the 5G NR standards. These standards include the use of millimeter wave radio, multiple-input and multiple-output (MIMO), and beamforming to increase bandwidth and capacity of the radio link. During the transition to 5G, the current 4G bands (below 1 GHz) will still be utilized along with bands in the 6 GHz range and the bands above 24 GHz.

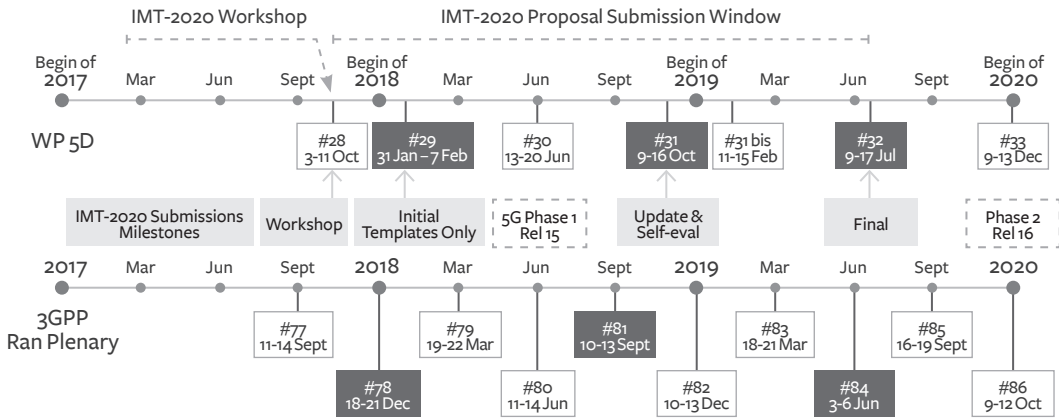


Figure 1: Timeline for 5G roll out and standards finalization. [19]

5G UE will also authenticate to the base stations differently using new authentication and key agreement methods (AKA). Where the UE authenticates will be important for the security analysis of 5G. Currently in 3G and 4G, mobile subscribers are equipped with Universal Subscriber Identity Module Cards (USIM) or colloquially known as SIM cards.[13] The idea for the use of USIM cards was for mutual authentication of UE to the networks it connects to in order to secure future communications.

5G architecture in standalone mode will include systems that will not be present in the current NSA model. The complete system will have eMBB, URLLC, and a massive Machine Type Communications (mMTC) like device-to-device communication. Mobile edge computing (MEC) will be added to the architecture in order to allow computational and storage intensive operations to be offloaded on these computing nodes attached to base stations.[21] This allows smaller hand-held and IoT devices to push graphic processing for augmented reality (AR) and other similar tasks to the network saving energy and CPU cycles.

5G will also be deployed using small cell radios. These access nodes operate in both licensed and unlicensed frequency spectra and have a range of 10 meters to several kilometers.[43] Due to the use of millimeter waves in the small cells, signal propagation is poor, therefore the distance radio waves can travel will be heavily limited, especially in densely populated areas.

To combat the issue of propagation, proposals have been made to integrate existing building wireless access, using the 2.4 GHz and 5 GHz IEEE 802.11 standards, to carry 5G data and allow UE equipment to connect to the cellular network without the need for extra equipment. Another feature of the 5G radios to help combat poor propagation is beamforming, a method of operating an antenna array to produce calculated signals that create constructive and destructive interference that form a concentration of signal in a specified location as represented in Fig. 2. Beamforming allows for improved signal and better data transfer speeds. The 5G networks will also include software defined networking (SDN) for hands-off, improved quality of service, and allowing device-to-device communications. With new architecture comes the ability to create much faster and more resilient networks. It also comes with challenges which are discussed in the next section.

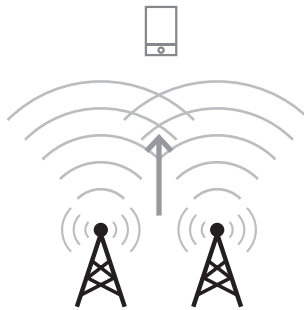


Figure 2: A basic visual representation of beam forming.

2.2 Challenges

With every new technology comes challenges that are inherent to the system or are newly introduced with the addition of features. Not all of the challenges faced are issues that will cause undue harm to the system. Some are merely items that, if left unattended, can cause the system to function erratically or cause further issues. Identifying these challenges ahead of time can have a significant positive impact on the total outcome of the introduced technology. In the case of 5G, there have been some items pointed out that need to be addressed before a stable system can be thoroughly vetted. With more devices being able to connect with the 5G network, there is a greater need for the ability to thwart attackers attempting to subvert authentication systems and causing a denial of service. These items are important to note and will be discussed below:

2.2.1 Trust Infrastructure

The architecture in 5G is based on a Public Key Infrastructure (PKI) system. A PKI system is one that uses cryptographic keys in order to establish identity. A public key and private key are created by a certification authority (CA) for each device. The private key should only ever be known to the device that needs an identity and the public key can be distributed to

any party that needs to encrypt messages to the device. The CA that creates these keys is trusted by all devices in the chain that need to check the validity of the certificates. When a device needs to connect, it will present a message signed by its private key to the authorization system. The authorization system will validate the message by decrypting it with the public key that corresponds to the private key of the device. The system will also verify that the public key it used was created by the trusted CA, so it knows the certificates are valid. If all these checks pass, the system will be able to confirm the identity of the device.

The PKI system is the current authentication mechanism in 4G with the cryptographic keys placed permanently on the USIM chips. The devices present their digital certificates to the base station, which then determines whether or not to allow the device on the network. Having permanent keys causes an issue when the number of UE increases substantially with the suspected adoption of 5G for IoT. If keys are compromised, carriers cannot reissue keys instantly. Replacing the USIM card is the only remediation for changing keys. In the current 4G space with an approximate 4.7 billion devices, it would be near impossible to replace even 10% of keys if a catastrophic event were to occur such as a breach that exposes the private keys of all the subscribers. Extrapolating to the proposed 5G space, that number becomes extremely large and even more unfeasible to handle. A solution would be a global adoption of a single large-scale PKI system.^[33] It would be the responsibility of each carrier to opt into the global PKI in order to create a usable and seamless system. The specifics of issuing, replacing, recovering, and revoking keys has already been drawn out by the Internet Engineering Task Force.^[15, 35, 23] The PKI system could also be used for devices to authenticate with each other before carrying out device-to-device communication that would not traverse through the carrier security equipment. Implementation could be baked into the 5G requirements and would add a significant layer of defense to the architecture.

2.2.2 Interconnection of Devices

One of the major milestones for 5G and one item of interest from mobile carriers is the introduction of IoT into the 5G space. IoT will allow for smart homes, smart cars, smart cities, or similar environments. These additions can make life easier in certain aspects; it also opens up the attack surface for abuse. There will now be more devices online and connected to the same network; this increases the number of potential eavesdropping devices, potential pivots for denial of service attacks, and potentially private data collection devices. If the current landscape of Industrial Control Systems (ICS) can be used as a guide, it should be noted that many of these devices very seldom get updates due to the need for thorough testing from manufacturers and end users.^[37] Updates have to be planned and scheduled weeks, if not months, in advance. A significant amount of ICS equipment runs on old or outdated operating systems that cannot be patched due to the lack of support by the vendor.^[37] Following that example would mean that many of these mass-produced devices will likely be left

without security updates and remain connected to home networks creating vulnerabilities and endangering the privacy and security of the people who live there.

3. SECURITY FOR 5G FEATURES

In the specifications for 5G, security was implemented at the beginning of its creation as all technologies developed in this day and age should strive to accomplish.^[2] This is important for a couple of reasons. First, planning to add security on top of a product that already exists doesn't produce the best results. Think of an entrance to a house. A door is used to keep the elements out and segment different spaces. If security is not thought about before installing the door, it is added on after. This could be in the form of a chain or a latch. While these two components can help, having installed the door with a deadbolt and a metal frame would have been far more effective. Of course, this doesn't prevent a person from breaking in through a window or the roof. Second, it is harder to get users and providers to accept the security changes if they are used to operating without them. If a person enters their home without a key and all of sudden needs to use and keep track of a key, it can be hard to convince the person that it is useful without breaking into their home. So, while security is incorporated in the beginning, it is important to look for holes in the protocols.

3.1 *HetNet*

A heterogeneous network, or HetNet, is a combination of different powered radio nodes that cover an area to provide high throughput for a large number of devices.^[39] In order to cover densely populated areas and areas with poor reception (e.g., office buildings, rural areas, intercity spaces, etc.), a heterogeneous network of cells is deployed to create coverage. An example of a HetNet is shown in Fig. 3. This network approach is an important feature of the 5G infrastructure. It will allow an extraordinary number of devices to connect and transfer large amounts of data that is not possible in the current LTE environment. HetNets allow for the ability to connect a multitude of devices and allow for the smart-enclaves.

Since endpoints connect to the strongest node with the highest signal-to-interference-plus-noise ratio (SINR), it is trivial to find the geographical region of a device. From Yang et al., adding randomness to the SINR can prevent determining the location of a device on a network.^[41] In a HetNet, there are high powered nodes (HPNs) and low powered nodes (LPNs). These nodes tend to overlap in high-density areas and can create a load balancing problem. Yang et al. propose incorporating security-oriented mobile association policies to monitor and balance the loads of HPNs and LPNs thus increasing the secrecy performance of the connection.^[41]

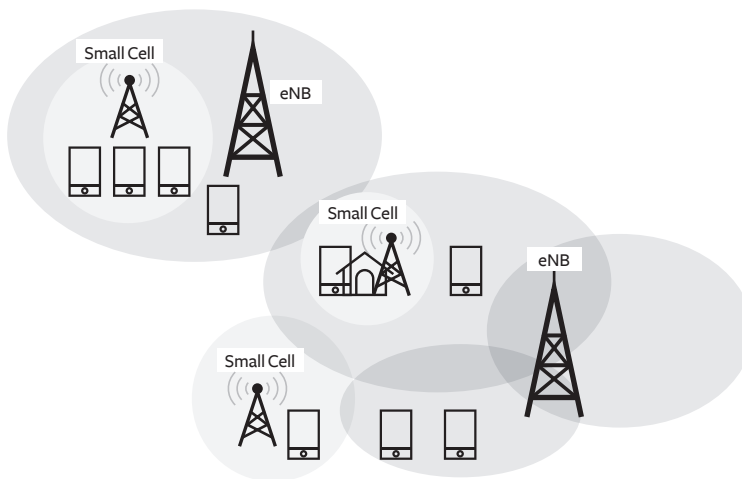


Figure 3: Illustration of a heterogeneous network.

3.2 Massive MIMO

Multiple Input Multiple Output (MIMO) is a technology that relies on several antennas to simultaneously transmit streams of data in wireless communications.^[31] MIMO is currently in use on consumer-grade wireless access points and in the current 4G LTE architecture as well as GSM and CDMA communications.^[26] Massive MIMO improves on its predecessor through the use of hundreds of antenna arrays allowing simultaneous access to several dozen endpoints in the same time-frequency domain.^[31] Massive MIMO can allow for increased capacity on the frequency resource, significant reduction of latency over the air, and increases resiliency to intentional and unintentional interference.^[31] Massive MIMO can produce beamforming as mentioned previously and allows for a shift in signal processing from the endpoint to the base stations (BS) and fits well within the specifications for 5G.^[20] Massive MIMO can also increase the security of a connection. According to Chen et al., when a base station has a large enough number of antennas the proposed original symbol phase rotated secure transmission scheme can defend against an attacker with an unlimited number of antennas from decoding the original symbols.^[14] This will keep a physical connection secure from eavesdropping.

3.3 Device-to-Device

The 5G standard introduces device-to-device communications (D2D). The purpose of D2D is to allow endpoints to communicate with each other without having to pass through base stations.^[20] Communication traffic will be offloaded from base stations since no connection to the network infrastructure is needed. A primary application for this technology is the use of vehicle-to-vehicle (V2V) communication to facilitate self-driving cars and collision avoidance messages.^[27] The V2V communication is also important for standard vehicles to communicate information to other drivers and even vehicles that are not self-driving. Security is a concern when allowing direct communication between UE. Taking into account all of the IoT devices that

will now be able to participate in D2D communications can cause concern. Several proposals attempt to improve the security of D2D communications. Ghanem and Ara produced a method of cooperation that takes into account distance between nodes as a security mechanism.^[22] If a device believes that a connection to another based on distance can increase security, then it can make that request. The other end of the connection also calculates the path and decides to cooperate or suggests moving to keep the confidentiality of the connection intact and help avoid eavesdropping. The use of distance as a security parameter helps keep the connection more localized without having to pass through more network hops than needed. Using fewer network hops limits exposure to other devices that are also listening, but it does not completely solve that problem. Another solution proposed by Ghanem and Ara introduces a security scoring system (SeS) for measuring the protection of a connection.^[7] The system calculates a score at the physical layer to detect attacks without needing to incorporate computation at higher levels of the software stack. The score produced is based on probabilistic characteristics of the transmitted data in a D2D connection. A few other solutions incorporate the use of a PKI system where devices create their own keys without the use of certificates. This form of verification would look more like a web-of-trust seen with PGP where devices verify each other removing the centralized management that is a single point of failure.

3.4 Software Defined Networking

Software Defined Networking (SDN) is becoming more popular as organizations move infrastructure to the cloud and virtualize the systems and applications that remain on-premise. SDN allows for the rapid implementation of routing rules and protocols to support an ever expanding and contracting network. In traditional networks, access control lists (ACLs) and routing statements need to be updated on every hop in a routing chain to allow for creations of new networks inside a large enclave. SDN solves this problem through centralizing the management of a network and allows for automation that can greatly expand the flexibility of a network and reduces workload. One of the solutions with 5G is the inclusion of SDN. With 5G, SDN will be needed to rapidly adjust routing between devices and automate the creation and modification of access control lists. It will allow for centralized management and facilitate D2D communication. Some potential for abuse comes with the centralized control plane. There is also still the ability to attack individual devices operating in the SDN. Some malicious behavior on SDNs and their causes are outlined by Dabbagh et al.^[17]

4. SUMMARY OF VULNERABILITIES

From the current published standards and research conducted in the 5G community, some notable vulnerabilities have come to light. These vulnerabilities can be addressed in future standards releases, and some are expected to have mitigations in place when 5G standards are finalized. The vulnerabilities addressed in this paper are broken down into three sections: Confidentiality, Integrity, and Availability (CIA). The CIA triad, as it is known, is the cornerstone of security policy and dictates the most crucial components of security. Some of the following

findings are hold overs from 4G LTE that have yet to be addressed in current published standards. It is likely that several of them will be addressed in the future, however, some of the findings will be difficult to mitigate and as of 3GPP Release 15, they are still vulnerable.^[33] An overview of security threats and their impact from this report can be found in Table 2.

Table 2: Summary of 5G Threats and Impacts

Security Principle	Threat	Impact
Confidentiality	AKA Attack Unsecured DNS Paging Broadcast	Spoofing Malware dropping MITM Location Determination
Integrity	Silent Downgrade AKA Attack	Phone/SMS snooping Subscriber Impersonation
Availability	Spectrum Slicing Attack Botnet Attack Paging Attack	Performance Degradation Denial of Service

4.1 Confidentiality

Confidentiality is the principle that sensitive data will be prevented from being released to parties that have no need or authority to access. In the case of cellular communications, that can mean text messages, phone calls, and internet traffic. In the 5G space with IoT, that can mean medical devices that collect data for practitioners or building control equipment that allows entry into an area. It is essential that this data be safeguarded from threats in order to prevent unintended leaks of personal or security data.

4.1.1 AKA Attacks

Authentication and Key Agreement (AKA) for 5G security and attacks are heavily researched in Borgaonkar et al, Basin et al., and Cremers and Dehnel-Wild.^[13, 11, 16] Privacy was built into the standard for 3G and 4G authentication.^[1, 3] Unfortunately, there have been weaknesses found in the AKA system that allows for false base stations attacks and IMSI catchers through non-protected identity request mechanisms and authentication failure messages.^[13] These flaws allowed for the creation of StingRays, a device used by law enforcement to track users through their cellular devices.^[42] The protocol is extremely important for controlling devices that are allowed on the network and maintaining the confidentiality of communications. From Cremers and Dehnel-Wild, the 5G-AKA protocol does not meet its own security requirements. It is shown that an attacker can access a service network in the name of a legitimate user other than itself.^[16] The attack is possible due to insecure transportation methods used to transfer secret keys between UE and a base station required for authentication while a device is roaming. A real-world application of the attack would be dependent on how the network carrier implements its authentication mechanism. There are other known attacks against AKA that have been inherited from the 4G protocol standards.^[13] In order for carriers to provide backward compatibility, the architecture from 4G will still be operational, and even while the

shift to 5G occurs, devices will still need to communicate with a 4G network first before being upgraded to 5G. In the current 5G AKA specification, a vulnerability was found that would allow an attacker to learn about the cellular consumption of a user through a replay attack from lack of randomness in the sequence number (SQN).^[13] The SQN can be thought of as a token that allows access to a resource. This has major privacy implications since an attacker will be able to determine the time spent on phone calls, SMS statistics, and some web traffic usage. This attack works even while a user is not in range of an attacker's fake base station since a device will update the statistics when it returns in range of the false base station. This could mean that an attacker could determine the location and schedule of a user while only knowing the target's phone number.

4.1.2 Man-In-The-Middle

In the 5G space, Man-in-the-Middle (MITM) attacks are mostly resolved in theory with two-way authentication for the UE and the base station as well as service providers that are in the middle. This can prevent a false base station from sniffing traffic of the UE that connect directly to it. However, a flaw in the 5G-AKA standard described in Section 4.1.1 will allow an attacker to reuse authentication keys from a previous session to create a false base station.^[11] This would open the door to surveillance devices, like the StingRay and other ISMI catchers that are used currently in LTE networks.

Aside from the issues with authentication, there has been research on the insufficient protection of DNS traffic.^[34] Intercepting or poisoning DNS entries can create a whole host of issues. Changing legitimate DNS requests to return malicious IP addresses can allow the attacker to perform MITM attacks, steal credentials, and deploy remote malware.

4.1.3 Location Discovery

A Temporary Mobile Subscriber Identity (TMSI) is a randomly assigned credential given to a device by a network operator's Mobile Management Entity (MME). It is recommended that the TMSI for a device should be changed frequently.^[24] However, in practice, this TMSI does not change often. When there are one or more pending services for a device, the MME asks a nearby base station(s) to broadcast a paging message, which includes the TMSI of the device. This makes the process of locating a device in an area a much simpler process. The attack involves determining the paging interval of a target through the use of sniffing traffic on the network and placing calls or texts at known times and allowing for a delay. The network will broadcast the paging notification and slowly an attacker can find the target device. Once the paging interval is known, a device can be tracked in any cellular area that the attacker has a sniffer in.

4.2 Integrity

Integrity is the principle of maintaining the accuracy and consistency of data from end point to end point, and it is important in wireless communications to prevent data from being

manipulated due to environmental factors or malicious actors. Wireless specifications often incorporate methods to re-transmit data in order to overcome disconnects or interference and to continue connections. It is important that this data is verified that it is exactly the same as what the device sent. The consequences for altered data accepted can be as benign as a glitch in a phone conversation to as catastrophic as power plants receiving the wrong control codes.

4.2.1 Message Alteration

In the current model, message authentication provides the verification of the source; however, there is no protection against the duplication or modification of the message.^[20] Data transfer is much easier to alter when compared to voice communications. Since much of the data transfer security is reliant on the application the device is communicating with, it is difficult to remediate in the 5G space.

4.2.2 Message Spoofing

From the AKA attacks in Section 4.1.1, an attacker can spoof a device on a cellular network. That will allow for the attacker to send SMS messages and phone calls as the subscriber they are impersonating.

4.2.3 Silent Downgrade

When a UE attempts to connect to a base station, there is a negotiation that occurs where the UE and base station determines authentication mechanisms, speeds, and encryption. A malicious base station may be able to force the UE to downgrade to GSM, an older and less secure communication protocol, exploiting the pre-authentication messages. All a false base station would need to do is broadcast a valid Mobile Country and Network Code (MCC-MNC) combination for a network that has no public key provisioned in the USIM. This will allow for MITM attacks, phone call snooping, and SMS message snooping.^[33]

4.3 Availability

Availability is the third leg of the CIA triad. This principle requires that all information systems be functional and accessible at all times. It is an important objective because, without availability, nothing else matters. If a system is not available, it is of no use to anyone. When dealing with cellular networking, an area being out of coverage can have major consequences. In this day and age, most users do not have landline telephones, and there are very few public telephones around. When life safety is involved, and communication is critical, the system that carries communications is vital.

4.3.1 DDOS

A distributed denial of service (DDOS) attack occurs when a malicious actor attempts to disrupt service to a commodity through the use of overburdening the system with fake requests and data traffic from a large number of devices. This attack is hard to circumvent and difficult to track down to a single root cause. In the 5G space, the inclusion of IoT will make this style

of attack much more devastating and potentially easier to orchestrate. Right now, there is not an abundance of non-mobile operating systems in the 4G LTE ecosystem, so the bar to abusing and compromising these devices is higher. When wireless cameras that are running on outdated versions of Linux with web servers becomes more common, it is not out of the realm of possibilities that an attack like the one seen with the Marai botnet will make its way to the 5G space.^[30] It is especially important to include DDOS protections and mitigations in the standards and for network operators to work to thwart such efforts.

Infrastructure. As stated previously in 3.4, having a 5G SDN can alleviate many foreseen problems with connecting a massive amount of devices to a network, but it also creates some single points of failure. The control plane and the individual switches in the core infrastructure are targets for attempts to disrupt service in a large area.[8] An attempt to locate the control plane for the SDN and go after individual network components can have major negative effects if not properly defended.

With radio spectrum being a scarce resource, the practice of leveraging unused radio frequencies in a geographical area to use for 5G communications is included in the 5G proposals. [28] Using the frequencies set aside for government operations can provide benefits in areas where there are many devices attempting to communicate over the same frequencies and causing connection issues.^[12] There is potential for abuse with this method when looking at how the 5G infrastructure handles off-loading the connections when a control signal from the military or government operations system attempts to broadcast on the reserved frequencies. If the equipment that is attempting to use the spectrum allocated for it cannot properly reach the 5G infrastructure to allow it to broadcast over the 5G equipment, then it can potentially cause a denial of service and hamper critical communications. More research will need to be done to determine how feasible that attack would be from a well-resourced threat actor.

User Equipment. As with the infrastructure, user equipment is vulnerable to DDOS conditions at an even higher rate. This equipment is likely not made to handle extremely high rates of data traffic. In current network topologies, these devices do not normally take the brunt of a network attack. Routing and switching equipment along with firewalls and intrusion prevention systems (IPS) will absorb most of a large DDOS attack by protecting the endpoints. In 5G with D2D communications, these devices are potentially exposed to such attacks from malicious actors that are in the vicinity of a target and have the capability to use other user equipment as a part of a botnet. From following previous attacks that are able to determine the location of a user, a threat actor can set up an attack using the devices in an area to launch against a specific target using the paging occasion hijacking discussed in 4.1.3. Preventing such an operation would be difficult unless a network operator could detect indicators of an attempt and perform mitigation.

CONCLUSION

This paper discusses the current landscape of 5G networking and security and attempts to bring all aspects of the environment together to create a thousand-foot view of the topic. There are many places where security can be built into the specification, where it currently is missing, or lacking specific details. As the 3GPP, ITU, and IETF work to produce the final specifications, there will undoubtedly be changes made and the network carriers will adjust their deployments to follow. It would be beneficial to revisit this topic when the final publications are made available and more carriers are involved in rolling out their versions of 5G networking. Since it is up to each carrier to implement the standards and core infrastructure, there will be variations in what is produced. From a security standpoint, trusting a standard will not be enough to determine the overall resiliency of a solution. Further testing will surely be done when 5G networks are more available. With the availability and relatively low-cost of software-defined radios (SDRs), testing these cellular networks will not be as difficult as it once was. As of now, there is no actual silver bullet that makes 5G unfeasible or wildly insecure. It will take time before all the standards in 5G are worked out and a stable system is produced. Until then, there should be some hesitation in using the 5G network for enterprise communications. ♥

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, or the Department of Defense.

Author Bio

Shane Fonyi

Shane Fonyi is a Cyber Research Integrator for the Army Cyber Institute at West Point (ACI). He is responsible for consulting with research teams at the ACI and other organizations to determine requirements and provide guidance on projects as well as developing and building the necessary IT infrastructure. He has been a speaker at several IT and Information Security conferences including BSides KC and the Conference on Higher Education in Kansas for work involved in IoT research and security awareness. He currently holds a Bachelor of Science in Electrical Engineering from The University of Kansas as well as several industry certifications including the CISSP, SSCP, CySA+, and GCFA. He is also an NYU Cyber Fellow at the NYU Tandon School of Engineering.

NOTES

1. 3GPP. 3G Security; Security Architecture. 15th ed. 3GPP, 2018. url: <http://www.3gpp.org/DynaReport/33102.htm>.
2. 3GPP. Security Architecture and Procedures for 5G System. Tech. rep. TR 33.501 V 15.4.0. 3GPP, Mar. 2019. url: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>.
3. 3GPP. Service Requirements for the Evolved Packet System (ETS). TS 122.278. 3GPP, 2018. url: <http://www.3gpp.org/DynaReport/22278-CRs.htm>.
4. 3GPP TR 21.915, "Release Description; Release 15". https://www.3gpp.org/ftp/Specs/archive/21_series/21.915/21915-100.zip. Accessed: 2019-04-19. 2018.
5. About 3GPP Home. Accessed: 2019-04-30. 2019. url: <https://www.3gpp.org/about-3gpp/about-3gpp>.
6. About International Telecommunication Union (ITU). Accessed: 2019-04-2019. url: <https://www.itu.int/en/about/Pages/default.aspx>.
7. I. Abualhaol and S. Muegge. "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns". In: 2016 49th Hawaii International Conference on System Sciences (HICSS). Jan. 2016, 5763–5771. doi: 10.1109/HICSS.2016.713.
8. Ijaz Ahmad et al. "5G security: Analysis of threats and solutions". In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE. 2017, 193–199.
9. Grudi Associates. The Facts about 3g, 4g & LTE Wireless Service. Grudi Associates, 2012. url: <https://grudiassociates.com/wp-content/uploads/The-Facts-About-3G-4G-LTE-.pdf>.
10. "Auction of Upper 37 GHz, 39GHz, and 47 GHz Bands Critical to Ensuring United States Leadership in 5G". In: (July 2019). url: <https://docs.fcc.gov/public/attachments/DOC-358397A1.pdf>.
11. David Basin et al. "A formal analysis of 5G authentication". In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM. 2018, 1383–1396.
12. S. Bhattarai et al. "An Overview of Dynamic Spectrum Sharing: Ongoing Initiatives, Challenges, and a Roadmap for Future Research". In: IEEE Transactions on Cognitive Communications and Networking 2.2 (June 2016), 110–128. doi: 10.1109/TCCN.2016.2592921.
13. Borgaonkar, Ravishankar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols." Proceedings on Privacy Enhancing Technologies 2019, no. 3 (2019): 108–27, <https://doi.org/10.2478/popets-2019-0039>.
14. B. Chen et al. "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper". In: IEEE Access 4 (2016), 3016–3025. issn: 2169-3536. doi: 10.1109/ACCESS.2016.2580673.
15. S. Chokhani et al. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647. RFC Editor, Nov. 2003.
16. Cas Cremers and Martin Dehnel-Wild. "Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion". In: Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi: 10.14722/ndss.2019.23394.
17. Mehjar Dabbagh et al. "Software-defined networking security: pros and cons". In: IEEE Communications Magazine 53.6 (2015), 73–79.
18. Jessica Dolcourt. Testing Verizon's early 5G speeds was a mess, but I'm still excited about our data future. 2019. url: <https://cnet.co/2V3Dzun>.
19. ETSI. 5G Timeline. 2019. url: <https://www.etsi.org/technologies/5g>.
20. D. Fang, Y. Qian, and R. Q. Hu. "Security for 5G Mobile Wireless Networks". In: IEEE Access 6 (2018), 4850–4874. issn: 2169-3536. doi: 10.1109/ACCESS.2017.2779146.
21. Alex Galis et al. Mobile Edge Computing – An Important Ingredient of 5G Networks. 2016. url: <https://bit.ly/2S5eyST>.
22. Samah AM Ghanem and Munnujahan Ara. "Secure communications with D2D cooperation". In: 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15). IEEE. 2015, 1–6.
23. R. Housley. Internationalization Updates to RFC 5280. RFC 8399. RFC Editor, May 2018.
24. Syed Rafiul Hussain et al. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information". In: Network and Distributed Systems Security (NDSS) Symposium 2019 (2019). doi: 10.14722/ndss.2019.23442.
25. Pablo Iacopino et al. The 5G era in the US. Tech. rep. GSM Association, 2018. url: <https://www.gsmintelligence.com/research/?file=4cbbdb475f24b3c5f5a93a2796a4aa28&download>.

NOTES

26. “IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput”. In: IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k- 2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009) (Oct. 2009), 1–565. doi: 10.1109 / IEEESTD.2009.5307322.
27. National Instruments. Applications of Device-to-Device Communication in 5G Networks. 2019. url: <https://spectrum.ieee.org/computing/networks/applications-of-devicetodevice-communication-in-5g-networks>.
28. T. Irnich et al. “Spectrum sharing scenarios and resulting technical requirements for 5G systems”. In: 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops). Sept. 2013, 127–132. doi: 10.1109/PIMRCW.2013.6707850.
29. IETF | Who We Are. Accessed: 2019-04-30. 2019. url: <https://www.ietf.org/about/who/>.
30. Brian Krebs. Who Makes the IoT Things Under Attack? — Krebs on Security. 2019. url: <https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/>.
31. Erik G Larsson et al. “Massive MIMO for next generation wireless systems”. In: arXiv preprint arXiv:1304.6690 (2013).
32. Minimum requirements related to technical performance for IMT-2020 radio interface(s). Accessed: 2019-03-26. 2017. url: <https://www.itu.int/pub/R-REP-M.2410-2017>.
33. R. Piqueras Jover and V. Marojevic. “Security and Protocol Exploit Analysis of the 5G Specifications”. In: IEEE Access 7 (2019), 24956–24963. issn: 2169-3536. doi: 10.1109/ACCESS.2019.2899254.
34. David Rupperecht et al. “Breaking LTE on layer two”. In: IEEE Symposium on Security & Privacy (SP). 2019.
35. S. Santesson et al. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 6960. <http://www.rfc-editor.org/rfc/rfc6960.txt>. RFC Editor, June 2013. url: <http://www.rfc-editor.org/rfc/rfc6960.txt>.
36. Statista. LTE subscriptions worldwide 2018-2023. 2019. url: <https://bit.ly/2JkOe1B>.
37. Keith A. Stouffer, Joseph A. Falco, and Karen A. Scarfone. SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC). Tech. rep. Gaithersburg, MD, United States, 2011.
38. The State of LTE (February 2018). Feb. 2018. url: <https://www.opensignal.com/reports/2018/02/state-of-lte>.
39. Jeanette Wannstrom and Keith Mallinson. HetNet/Small Cells. 2019. url:<https://www.3gpp.org/hetnet>.
40. Cisco Wireless. 5G Non-Standalone Solution Overview. Accessed: 2019-04-2018. url: https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-5_NS-8/5G-NSA/21-5-5G-NSA-Solution-Guide/21-5-5G-NSA-Solutions-Guide_chapter_01.pdf.
41. Nan Yang et al. “Safeguarding 5G wireless communication networks using physical layer security”. In: IEEE Communications Magazine 53.4 (2015), 20–27.
42. Kim Zetter et al. Florida Cops’ Secret Weapon: Warrantless Cellphone Tracking. 2014. url <https://www.wired.com/2014/03/stingray/>.
43. Haijun Zhang et al. “Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum”. In: IEEE Communications Magazine 53.3 (2015), 158–164.

Deciphering Cyber Operations

*The use of methods and simulations
for studying military strategic
concepts in cyberspace*

Seth T. Hamman
Jelena Vičić

Jack Mewhirter
Philip White

Richard J. Harknett

ABSTRACT

The academic research community faces a significant hurdle when it comes to the study of nation-state cyber operations dynamics. For national security and commercial reasons, little to no cyber operations data is disclosed to the public. Without access to operational data, academic contributions will remain inhibited and the academy will be underutilized in the study of this important strategic domain. We claim that researchers can begin to overcome this information gap by designing experiments that take place within simulation environments. Such approaches are beneficial in that they allow researchers to generate data not easily collected or observed in real-world settings and increase the capacity of researchers to isolate causal effects. In this paper, we describe a simulation environment specifically designed to study cyber operations dynamics below the threshold of armed attack—the competitive space where nearly all nation-state cyber operations activity takes place today. We discuss the simulation environment and then, to illustrate how it can be leveraged to generate tests of research hypotheses, detail our pilot experiment which examines the escalatory dynamics of defend forward activities.

I. INTRODUCTION

The National Security Strategy of the United States (NSS) acknowledges, “today cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing the border.”^[1] The Department of Defense National Defense Strategy (NDS) designates cyber as a foundational capability under its Global Operating Model and sets the expectation that cyber operations will be “designed to help us compete more effectively below the level of armed conflict.”^[2]

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Both of these central national documents, along with U.S. Cyber Command's (USCYBERCOM) Vision document and Department of Homeland Security Cyber Strategy expand the focus of cyber operations beyond contributing technically to wartime missions (the focus of previous policy) to include both defensive and offensive capabilities and actions that can delay, degrade, and deny an adversary's ability to produce cumulative effects below the threshold of war that can create strategic advantage.^{[3][4]} According to Lt. Gen. Bruce T. Crawford, U.S. Army Chief Information Officer/G-6, "The bottom line, when it comes to the threat, is that never again will we have the luxury of operating in uncontested space. That's become a part of who we are now."^[5]

The academic community faces a significant challenge to contribute empirically-based research findings relevant to this new, more active approach in cyberspace. For national security reasons, most government cyber operations remain classified. Operations involving the private sector are rarely discussed in detail due to commercial concerns. Thus, the empirical record rests primarily on after-action reporting through third-party commercial entities, general news reporting references, or broad attribution of prior attacks. The operations themselves remain opaque and generally unobservable to the academic community in real-time.^[6]

The lack of available data constrains academic contributions to the field of cyber operations and conflict. A significant portion of research under the heading of "cyber operations," therefore, tends to focus on technical innovations that are developed under capabilities requirements. While this contribution is essential, it remains too narrow to improve the US position regarding the ongoing cyber campaigns waged against US national sources of power to which the NSS calls attention. Strategic considerations must set and shape technological advances. Without a robust mechanism to generate unclassified, unbiased data about the dynamics associated with cyber operations, academic research will remain constrained by the limits of deductive analysis and limited heuristic case study. In other words, security studies scholars, in particular, have to rely on the security firms' research and reporting by journalists, as well as on heuristics, to make sense of opaque case studies in the absence of unclassified reports.

In this paper we discuss how researchers can utilize experimental research designs and simulation environments to produce unique datasets that allow them to better examine cyber operation dynamics, and potentially, evaluate the efficacy of various cyber strategies. Such approaches may be potentially advantageous even if more observational data were made available, given the high potential of bias introduced through non-random case selection, measurement issues/errors, as well as spurious and/or endogenous relationships between outcome and predictor variables. We then illustrate how such a research design could be employed. We describe a computer environment created to simulate an iterated exchange between two cyber actors (one human player, one computer player). The computer is programmed to employ predefined actions which mimic different cyber strategies: by randomizing computer actions and observing actor response, we are able to evaluate how and to what extent various strategies elicit different types of responses.

Experimental approaches similar to the one described in this paper have long been utilized across various natural and social science disciplines to generate data not easily collected or observed in a natural setting and increase the capacity of researchers' ability to isolate causal effects. Leveraging this established approach and bringing it into the subfield of cyber security studies will help usher in a new range of academic contributions. This project is the first critical step to create that foundational method and we hope to contribute directly to the concerns of the NSS and NDS on how adversary behavior is threatening "the safety of the American people and the Nation's economic vitality."^[7]¹¹

In this paper, we describe approaches to the study of cyberspace and provide background on experimental methodology and wargaming. We then describe our simulation environment, which incorporates some core elements of wargaming. Lastly, we illustrate how experiments can be embedded within the environment to study meaningful questions by detailing our pilot experiment which examines the escalatory dynamics of defend forward activities.

2. RELATED WORK

2.1. Limitations to the Study of Cyber Conflict

The lack of cyber-phenomena-related data inhibits the academic study of cyber conflict. The cyber conflict literature has been stalled in its formative stages due to researchers' inability to create datasets with the full methods and research design toolkit (otherwise available to political scientists and international relations scholars).^[8] A study examining the methodological state of the field finds that out of the total number of 70 articles on cyber conflict published between 1990 and 2018, only 9 explicitly discuss their methodology.^[9] In almost three decades, not only have there been very few articles focusing on cyber conflict, but the articles that were published suffered from limited or no data. Moreover, there has been a strong focus on theory-building versus theory-testing articles, and both qualitative and quantitative approaches to the study of cyber conflict remain limited.^[10] As stated elsewhere, "[t]he need for a more scientifically structured approach is readily apparent to the [academic] community."^[11] Overall, the history of cyber studies is plagued with challenges, including a lack of comprehensive case studies and a small number of large n-datasets, as well as high levels of secrecy that inhibit research across different topics.^[12] Specifically, we were only able to identify two articles to-date on cyber conflict relying on quantitative data.^[13]^[14]² The challenge in studying events that are veiled in secrecy is that datasets are not complete and do not represent the whole universe of cases/events of cyber conflict. As such, biases are likely introduced by the limited number of cases that are represented in the sample. For example, only certain classes of cases may be reported by the media or uncovered by security researchers studying cyber conflict.

2.2. Experimental Methods

Capturing the impact that cyber operations strategies (e.g., persistent engagement) have on

¹ It is important to note that while our research questions in terms of strategy were informed by the American policy shift of 2018, the experimental model developed here can be applied to any state actor's strategy.

² While quantitative in approach, these studies still rely primarily on the opaque access to real world cases discussed above.

specified outcomes (the rate at which an entity is subject to cyber-attacks, one's resilience to cyber-attacks, the risk of escalation, etc.) is a complicated task. Notably, cyber operations come "with high degrees of anonymity and with plausible deniability; [...] more uncertain in the outcomes they produce; [...] and involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of seconds to years."^[15] As evidenced through the Rubin causal model, measuring the impact that a given strategy or policy has on a specified outcome requires that one observe outcome measures for a given unit (e.g., a country, a cyber-operator) across instances when that policy is enacted and when the policy is not enacted at the same time.^[16] For example, if a researcher is interested in evaluating how the defend forward operational concept may impact the rate by which a country is subject to cyber-attacks, one must simultaneously observe the rate at which a country is attacked when that operation is underway and when it is not. The difference between the outcome measures across these two conditions is defined as the "treatment effect" or the "causal effect" of a given policy. Our inability to observe a person/entity at more than one state at a time is known as the "fundamental problem of causal inference," which limits our ability to quantify causal effects.^[17]

For this reason, experimental methods have played a significant role in advancing the natural sciences and various social science disciplines, including, but not limited to: psychology, behavioral economics, and political science.^{[18][19][20][21][22]} Such approaches are beneficial in that they allow researchers to generate data not easily collected or observed in a real-world setting and increase the capacity of researchers to isolate causal effects. In essence, social science experiments are meant to replicate—and analyze variation between—how individuals behave when assigned to one of two or more conditions. Each condition is meant to simulate an alternate real-world environment; for example, when the defend forward operational concept is in effect and when it is not. Because individuals are randomly assigned to groups, on average groups share the same characteristics (e.g., ethnicity, sex, abilities, etc.): the only difference is the experimental condition to which they are subject.^[23] Because of this, the researcher can be assured that any difference observed in outcomes is *caused* by the treatment effect.

While experimental approaches are advantageous in that they allow the researcher to avoid the problems associated with unobserved counterfactuals and lack of access to real-world data, the extent to which findings can be generalized to the real-world is a function of how well the conditions replicate the real-world environment, and the extent to which treatment effects (again, variation in outcomes between treatment and untreated groups) observed in the sample are consistent with the population of interest (e.g., cyber operators, nation-states, etc.). As the simulation environment deviates from real-world conditions, and as samples differ from the population of interest, the likelihood that patterns of behavior accurately capture reflect real world processes decreases.^{[24][25]}

2.3. Wargaming

In the words of Thomas Allen, "Wargaming is a simulation of war, a horror show without

props.”^[26] It is an exercise envisioned to test, practice, and improve military strategies. An important aspect of wargaming is the realism of the exercise. Modern war games stress realism, as opposed to focusing on theory, and are useful in producing military contingency plans. According to Allen, “Real war games are blueprints of real war.”^[27]

The first “game center” in the US was operated by the Department of State in 1948, while wargaming was used as a military exercise all throughout the Cold War. From being played only by military personnel, wargames spread to universities such as MIT, and transformed into civilian military-politico exercises involving game theory.^[28] Historically, variables of interest in wargaming were related to institutional, cognitive, tactical, and strategic conditions and their effects on decision-making.^{[29][30]} More recently, wargames have been integrated into inexpensive digital game frameworks and new cloud computing architectures.^[31] This has paved the way for science-based experimental methods to be combined with wargaming models to produce large datasets for quantitative analysis. In its original form, wargames “examine the processes of warfare and do not present quantitative analysis of military effectiveness.”^[32]

In the context of cybersecurity, wargaming is mostly used by security firms in anticipation of cyber threats and incident response planning. The first government-led cybersecurity exercise was operated by the Department of Homeland Security in 2006. Named Cyber Storm, it was designed to test “response, coordination, and recovery mechanisms in reaction to simulated cyber events,” between international, federal, and state governments.^[33] In academia, the Naval War College focuses on testing decision-making processes involving “students, academics, and military thinkers,” rather than dynamics of conflict.^[34] Academic studies which analyze cyber-related wargaming data are rare. The only existing academic study involving cyber-related wargames is a longitudinal analysis of the escalatory nature of cyber operations using data from wargames played at Naval War College between 2011 and 2016.^[35] However, combining wargaming with replicable experimental design can be a useful tool for studying the dynamics of interactions in cyberspace that go beyond testing the decision-making processes in crisis situations.

3. THE SIMULATION ENVIRONMENT

3.1. Our Approach

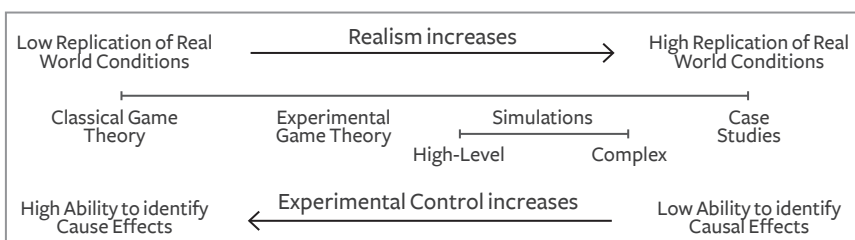


Fig. 3-1: The spectrum of scholarly research types for proposed national defense strategies.

The spectrum of potential scholarly support for proposed national defense strategies ranges from purely theoretical to case study-based (see Fig. 3-1). Theoretical approaches, as in classical game theory, are based on presuppositions such as player-perfect rationality and the presumed utility values of the players. This idealized environment enables mathematically-based deductions to be made and can forecast how players will respond in novel situations, assuming that all presuppositions are valid. Case studies, on the other hand, work inductively from real world examples, trying to identify salient characteristics and variables so that broadly applicable generalizations can be made and applied going forward.

In the case of cyber operations, both of these scholarly approaches are problematic. The presuppositions inherent in game theoretical models are likely to be questioned and (perhaps, rightly) distrusted because the domain is novel. As for case studies, the necessary numbers are not readily available for study both because the domain is new and access to existing cyber operations data is unavailable.

Our approach lies in the middle of this spectrum (see the “High-Level” marker in Fig. 3-1). We created a simulated cyber operations environment where data can be generated from diverse populations of research subjects on demand. Generating data from human subjects allows us to limit the number of assumptions that must be made regarding the players and their utility values, and we retain some of the dynamics of real-world cyber operations while still being able to identify causal effects by embedding experiments within the simulation environment.

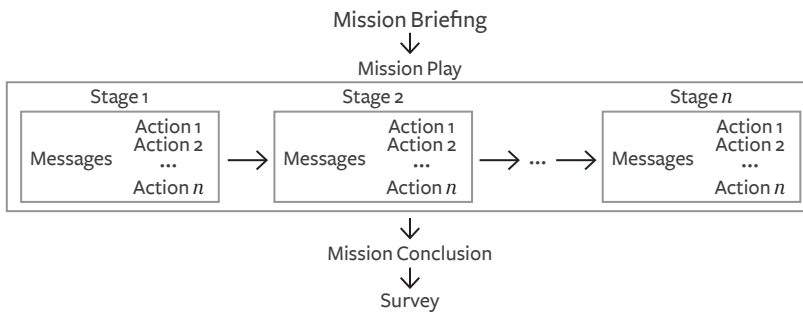


Fig. 3-2: The design of scenarios in the simulation environment.

The environment is a computer game that places research subjects in the role of a nation-state cyber actor. The research subjects participate as monads—each research subject plays against the computer. The research subjects log into the simulation via a web browser from any network-connected computer, and are presented with a *scenario* (see Fig. 3-2). Scenarios start with a *mission briefing*. In the mission briefing, the research subjects are charged with conducting a cyber operation against their adversary which may be modeled after a documented nation-state cyber operation. Details are changed to minimize the risks of research subjects playing out a known script. The mission briefing contains realistic but fictitious background information to contextualize the scenario with the goal of creating intrigue and buy-in from the research subjects. For example, they may be provided with information regarding their country’s economy

and military strength as well as that of their adversary's, and the scenario may include graphics such as a national seal or flag. These details may be modeled after actual nation-states, but fictitious names are used to avoid any potential psychological associations which could bias the research subjects' actions.

After the mission briefing, the *mission play* unfolds in *stages*. Stages have two elements: informational *messages* to provide the research subjects with situational awareness, and a set of *actions* related to the mission and its progress. In each stage the research subjects are tasked with selecting an action from the choices provided. When their choice is submitted, the next stage begins. The number of stages is variable and is determined by the study designer. The messages allow the study designer to inform the research subjects of the results of their previous actions as well as to update them about adversarial actions against their own network. Missions end with a *mission conclusion*—a final message that can be used to inform the research subjects of the overall results of the mission. At the conclusion of the simulation, the research subject can be presented with an optional *survey* to gather additional data.

The environment is a high-level simulation. The research subjects are not required to actually know how to technically conduct any of the steps of a cyber operation. For example, instead of having to manually run a Nmap network scan, the research subjects can just select the “Conduct Nmap network scan” action from the list of choices provided. In the next stage, they can be informed of the results of previous choices at whatever level of detail the study designer desires. This type of simulation sacrifices realism, but it accelerates the collection of data, and it lowers barriers to participation since trained expertise is not required. Therefore, in addition to technically trained and skilled cyber operators, non-technical managers and strategy-level personnel can participate in the experiments.

To help achieve realism, the stages of the operation are graphically mapped to the “cyber kill chain.” First developed by Lockheed Martin in an effort to improve network defense, the Lockheed cyber kill chain “describes phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering.”^[36]

Because the environment is a high-level simulation, it cannot be used to capture operational nuances such as inadvertent effects that may occur in a real-world mission. However, player reactions to unforeseen events can still be studied through the use of messages. For example, a message could be used to inform research subjects of an unintended consequence of one of their actions (e.g., “Your Nmap scan created a denial of service condition on the enemy network”).

The primary benefit of the high-level simulation design is that it allows the environment to be constrained to the exact specifications of the study designer. This allows all of the variables to be held constant except the treatment effect under study. This is vital for making causal inferences because as the level of realism increases in a simulation, confounding variables provide alternate explanations of the behavior observed, and this undercuts the study's

ability to identify statistically significant causal effects. Of course, high-level simulations have limitations as well (see Section 4.3), but they can still be an important component of the study of complex phenomena.

3.2. Technical Details

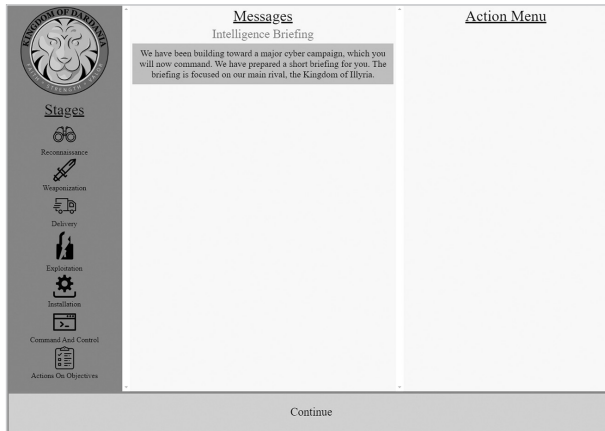


Fig. 3 3: The mission briefing screen in the simulation environment.

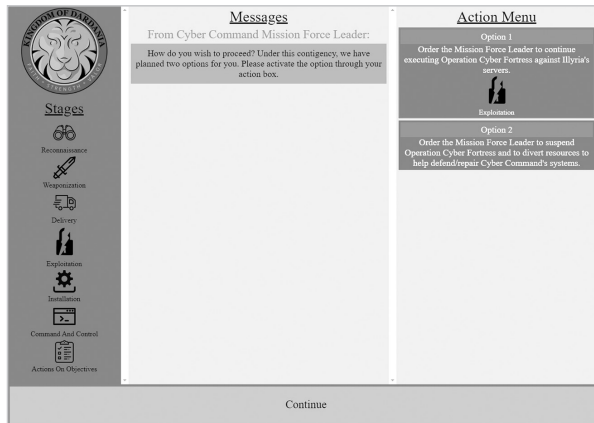


Fig. 3 4: The mission play screen in the simulation environment.

What is your academic standing?
Freshman
Sophomore
Junior
Senior
Graduate student
Not a student
Answer the Question

Fig. 3 5: The survey screen in the simulation environment.

The simulation environment is a client-server web application (see Figs. 3-3, 3-4, and 3-5). The application is highly customizable within a framework of scenarios as outlined in the previous section. The research subjects access the scenarios via any network-connected computer by browsing to a specified IP address and port number. The environment supports all standard web browsers. The server application is designed to be hosted on a research administrator's laptop and has a user-friendly graphical user interface (GUI). Client load demands are minimal so hundreds of research subjects can be served from a commodity laptop.

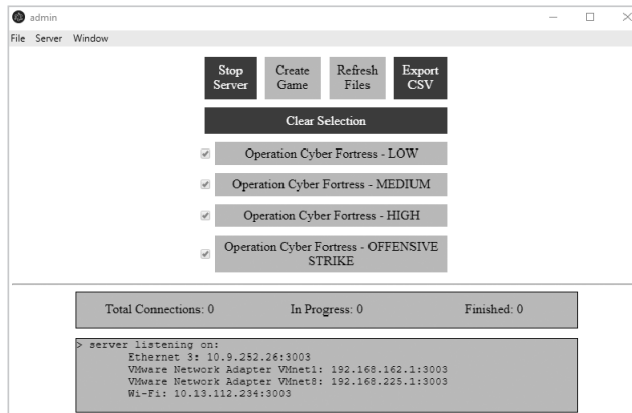


Fig. 3 6: Scenario administration: selecting scenarios and starting the server.

We designed the experimental environment to be highly portable. A typical data collection scenario may look like the following: a research administrator walks into a room with a laptop, connects to the Wi-Fi access point, starts the scenario server on the laptop with the click of a button, and announces to the research subjects the IP and port number where they can access the environment (see Fig. 3-6). The research subjects then connect to the server from the web browser of their choice. The research administrator can monitor which scenarios are being served and the status of the clients. The data clients generate is saved to the research administrator's computer for later analysis. Alternatively, the simulation environment can be hosted in the cloud like a typical web application which would allow access from any Internet connected computer.

The environment is built on Electron. “Electron is an open source library developed by GitHub for building cross-platform desktop applications with HTML, CSS, and JavaScript. Electron accomplishes this by combining Chromium and Node.js into a single runtime and apps can be packaged for Mac, Windows, and Linux.”^[37] We chose Electron because of its versatility and portability, and because all coding is done in JavaScript which is a very popular and well-documented programming language.

DECIPHERING CYBER OPERATIONS

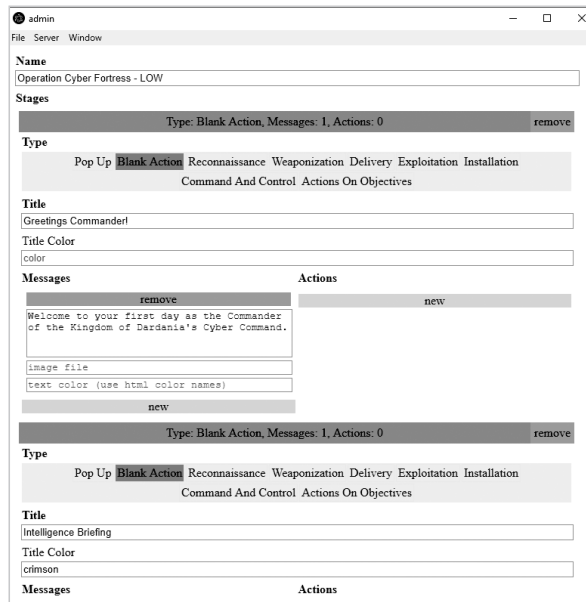


Fig. 3 7: Scenario administration: the scenario builder.

Our primary goal was to make the application as user-friendly as possible for the research administrators. The application package is distributed via a zip file, and can be unpacked on Windows, Linux, and Macintosh computers. Once unpacked, research administrators can use the GUI to create, edit, and delete scenarios (see Fig. 3-7), serve scenarios to research subjects as outlined above, and export the collected experimental data to a comma-separated values (CSV) file for analysis.

4. EMBEDDING EXPERIMENTS WITHIN THE ENVIRONMENT: OUR PILOT STUDY

In this section we provide an example of how experiments can be embedded within the environment. Our study, detailed below, seeks to examine the potential escalatory or non-escalatory dynamics associated with possible defend forward activities.

4.1. *The Interaction versus Escalatory Dynamics of Defend Forward Operations*

The careful study of the interaction dynamics of nation-state cyber operations is critical because the stakes are high—no country wants to risk inadvertently provoking another into a costly conflict. However, in this new technological paradigm, much uncertainty exists because there are few precedents. Real-world cyber operations data is not widely available, and even if it was, the relative scarcity of data points as well as the unique dynamics of any given data point would make it difficult to generalize the results.

The USCYBERCOM operationalized approach of persistent engagement, which positions cyber operators to defend forward and to actively contest cyber adversaries, is a significant pivot

in US cyber strategy and operations. It moves the emphasis from reacting to cyber intrusions to a more anticipatory footing with an emphasis on shifting the balance of initiative so as to keep US networks and data safer. ^{[38][39]} However, a defend forward posture involves continually conducting cyber operations on the computer networks of adversaries and, according to its critics, has the potential of provoking adversaries into an escalatory conflict. ^{[40][41]} At this early stage in the history of nation-state cyber competition, there exists little open-source evidence in either support or refutation of this claim. Therefore, the initial research questions we are investigating for our pilot experiment is:

Under what conditions does persistent engagement, which positions cyber operators to defend forward and actively contest cyber adversaries, lead to escalation to armed conflict or intensification of cyber interactions?

In order to study this dynamic, we created a set of scenarios based on published reports of state interaction in cyberspace, while integrating experimental design and war gaming into a simulation environment.

4.2. Experimental Details

Upon logging in to the simulation environment, the research subjects are informed that they are to engage in a cyber operations campaign against an adversary that their initial mission is to launch a spearfishing attack. The subjects are randomly assigned to one of four groups. All four groups are presented with the same mission. The initial stages, messages, and actions are also the same. The groups differ only in the final stage of the scenario as the messages reveal different degrees of defend forward activity that has taken place against the research subject's home network. This variation is the treatment effect that is used to determine how defend forward activities affect the final action selected by the research subjects. We designated the four groups as Defend Forward Low, Defend Forward Medium, Defend Forward High, and Preemptory Strike. The fourth variant is not a defend forward activity but is included as an experimental control to differentiate reactions to defending forward from reactions to a clear (non-inadvertent) adversarial escalatory behavior.

Experimentally, we designate each of the actions presented in the final stage as either escalatory or non-escalatory. We define activities directly related to carrying out the mission and to the defense of the home network as non-escalatory, and offensive activities not directly associated with the carrying out of the mission as escalatory. The last action the research subjects choose is the data point we are studying for this experiment.

This game set-up allows us to examine whether and at what level of intensity defending forward leads to escalatory or non-escalatory responses. Specifically, we can analyze whether increases in the intensity of the defending forward strategy (moving from Low to High) impacts the probability that a respondent chooses an escalatory response or remains in an interactions mode. It also allows us to disentangle at what level of intensity this increase might occur.

Given that subjects are randomly assigned to a given condition (meaning that on average, actors share similar qualities across groups), we can be assured that different propensities to escalate conflict across groups are solely due to treatment effects. We assure balance across groups by comparing demographics across groups. Various pre-estimation balancing techniques (e.g., coarsened exact matching) can be employed, if needed.

4.3 Pilot Limitations

The extent to which our study will provide generalizable information is contingent on the extent to which i) the behavioral patterns observed by study participants parallel those of the population of interest (for example, Russian cyber actors), and ii) our experimental conditions mimic real-world conditions. Here, we address each of these issues.

With regard to the first issue, it is important to note that we are concerned with treatment effects, not the underlying probability of escalation in any treatment or control group. While the sample population (in our case, initially students and eventually US cyber professionals), may differ in many ways that impact the underlying likelihood of choosing an escalatory response (risk aversion, training, culture, etc.) in any given scenario, it is less clear as to why the treatment effects would vary significantly if played by students or professional military personnel. A key difference could be that the sample and target population vary in terms of restraint: when subjected to more aggressive tactics, those with less restraint should be more likely to choose an escalatory option. If cyber operatives, on average, possess more or less restraint than those in our sample, our findings may under or overstate the escalatory effects of defending forward. Researchers should be careful to detail how differences between sample and target populations may impact between group variation when interpreting results.

With regard to realism, things become a bit trickier. In the real-world, cyber operators *generally* work within the context of an organization (in our case, the military). Organizations have institutionalized practices and norms that guide the way the actors respond. We believe that this is a valid subject question to tackle. Organizations are composed of individuals that have unique incentive structures and who possess some level of discretion when making a given choice. When engaging with an adversary, operators have preferences that are then modified by the organizational incentives.³ The strength by which preferences are modified vary across operators. Actors that prioritize their personal preferences may deviate from what is seen as organizationally correct, which in turn can have a profound impact on the organization as a whole. In military environments, rules of engagement can be expected to channel the behavior of individual operators. In our initial design, we capture a conservative rule of engagement in that the cyber commander making the decisions cannot escalate to conventional war directly, but rather can advise the central decision-maker (a king) to declare war and move to kinetic military operations. A looser rule of engagement can be modelled easily by changing this choice to a direct decision to respond to a cyber-attack with a kinetic attack. For this first design, we stayed with-in public reporting expectations about US rules of engagement. In this instance,

3 That said, organizational culture and norms have been found to shape the goals and preferences of individual members. This effect tends to vary across organizations and across members in the same organization.

if specific types of defending forward strategies elicit particularly high rates of escalation they perhaps should be avoided (given the propensity to elicit strong personal reactions) knowing well that said reactions will generally be modified. In future iterations of our model we will seek to capture the more fluid real-world environment of interactions across a range of cyber operations to test the potential of inadvertence under more complex testing environments.

5. CONCLUSION

Cyber insecurity is not going away anytime soon. We need to marshal a much broader range of academic expertise and empower it with new research tools so that the technical advances we make are set against real and expected adversarial behavior. This research project is a step in that direction.

At the end of the Second World War, the academic community was harnessed with providing technical, tactical, operational, and strategic guidance to deal with the security implications of the nuclear revolution. We need to once again harness a broad spectrum of academic researchers from across the technical computing and social sciences to pull back the veil of the unexplored security dynamics that have emerged and will continue to emerge in and through cyberspace. The dynamics of cyber operations pose a daunting challenge for states as they face a congested and contested strategic cyberspace domain. Our simulation environment provides a much-needed foundation to leverage unclassified, unbiased, empirically driven academic research to advance interests in an open, global, secure, and stable cyberspace. ♥

ACKNOWLEDGEMENT OF GOVERNMENT RIGHTS AND SPONSORSHIP AND DISCLAIMER

This project is sponsored by the National Security Agency under Grant Number H98230-18-1-0336. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein. This manuscript is submitted for publication with the understanding that the United States Government is authorized to reproduce and distribute reprints. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Security Agency.

Author Bios

Seth T. Hamman

Seth T. Hamman, Ph.D., CISSP, GPEN, CEH, GLEG, is the Director of the Center for the Advancement of Cybersecurity at Cedarville University and an Associate Professor of Computer Science. He earned his B.A. degree in Religion from Duke University, his M.S. degree in Computer Science from Yale University, and his Ph.D. in Computer Science with a specialization in Cybersecurity from the Air Force Institute of Technology. His research interests include helping to shape the growing academic discipline of cybersecurity and collaborating across the multidisciplinary spectrum of cybersecurity.

Jelena Vičić

Jelena Vičić is a Ph.D. candidate in the Department of Political Science at the University of Cincinnati, focusing on international relations, methodology, and cyber strategy studies. She holds the Master of Advanced International Studies (MAIS) degree from the Diplomatic Academy of Vienna. Jelena's research examines the patterns of state strategic behavior in cyberspace.

Jack Mewhirter

Jack Mewhirter is an Assistant Professor in the Department of Political Science at the University of Cincinnati. His research focuses on cooperation problems and influence in polycentric governance systems. Most of his work is done in the context of regional water governance systems.

Philip White

Philip White is an undergraduate Student Fellow in the Center for the Advancement of Cybersecurity at Cedarville University. He is pursuing a specialization in cyber operations within the B.S. in Computer Science major. At Cedarville, he is a member of the Cyber Competition Team and the ACM Programming Contest Team. After graduation, he hopes to pursue a Ph.D. in computer science.

Richard J. Harknett

Richard J. Harknett is Professor and Head of the Department of Political Science and Chair of the Center for Cyber Strategy and Policy at the University of Cincinnati. He co-directs the Ohio Cyber Range Institute. He served as Scholar-in-Residence at US Cyber Command and National Security Agency and in Fulbright Scholar appointments in Cyber Studies (Oxford University, UK) and International Relations (Diplomatic Academy, Vienna, Austria). He has authored over 50 publications in the areas of international relations theory, international security, and cyber security studies.

NOTES

1. White House, "National Security Strategy of the United States," 2018.
2. Department of Defense, "Summary of the National Defense Strategy," 2018.
3. Department of Defense, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber," 2018.
4. Department of Homeland Security, "Cybersecurity Strategy," 2018.
5. Geoffrey Dobson, Anushul Rege and Kathleen Carley, "Virtual Cyber Warfare Experiments Based on Empirically Adversarial Intrusion Chain Behavior," Ed. Leenen, Louise. *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (2018).
6. Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*, New York: Oxford University Press, 2018.
7. White House, "National Security Strategy of the United States," 2018.
8. Max Smeets and Robert Gorwa, "Cyber Conflict in Political Science: A Review of Methods and Literature," Working Paper Prepared for 2019 Annual Convention.
9. Ibid.
10. Ibid.
11. Thomas E. Carroll, David Manz, Thomas Edgar, and Frank L. Greitzer, "Realizing Scientific Methods for Cyber Security," *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results*, New York: ACM, 2012, 19-24, DOI=<http://dx.doi.org/10.1145/2379616.2379619>.
12. Max Smeets and Jason Healey, "Cyber Conflict History." *Cyber Conflict State of the Field Series: Economic Dimensions of Cyber Conflict*, Cyber Conflict Studies Association, 2017.
13. Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11." *Journal of Peace Research* 51, no. 3, May 2014, 347–360. doi:10.1177/0022343313518940.
14. Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (Feb 2019), 317–347.
15. William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds.) "Excerpts from Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," National Research Council, 2009.
16. James N. Druckman, "The power of television images: The first Kennedy-Nixon debate revisited." *The Journal of Politics* 65, no. 2 (2003), 559-571.
17. Paul W. Holland, Clark Glymour, and Clive Granger, "Statistics and Causal Inference," ETS Research Report Series, 1985.
18. Hal Pashler (Ed.), *Stevens' Handbook of Experimental Psychology, Volume 2, Memory and Cognitive Processes*, Hoboken: John Wiley & Sons, 2004.
19. John Duffy, "Macroeconomics: A Survey of Laboratory Research." *Handbook of Experimental Economics Volume 2*, by J.H. Kagel and A.E. Roth (Eds.), Princeton: Princeton University Press, 2016, 1-90.
20. A. E. Roth, "Introduction." *Handbook of Experimental Economics*, by J.H. Kagel and A.E. Roth (Eds.), Princeton: Princeton University Press, 1995, 1-110.
21. Rose McDermott, "Experimental Methods in Political Science." *Annual Review of Political Science* 5, no. 1 (2002), 31-61.
22. Samuel J. Eldersveld, "Experimental Propaganda Techniques and Voting Behavior." *American Political Science Review* 50 no. 1 (1956), 154-165.
23. Jasjeet S. Sekhon, "The Neyman-Rubin Model of Causal Inference and Estimation Via Matching." *The Oxford Handbook of Political Methodology* (2008).
24. David O. Sears, "College Sophomores in the Laboratory: Influences of a Narrow Data Base on Social Psychology's View of Human Nature." *Journal of Personality and Social Psychology* (1986), 515-530.
25. 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?" *Journal of Conflict Resolution* 50 no. 5 (2006), 757–776.
26. Thomas B. Allen, *War Games*, McGraw-Hill Book Company: 1989.
27. Ibid.
28. Ibid.
29. Ibid.

NOTES

30. Jacquelyn Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict." Thesis, The George Washington University: 2017.
31. Andrew W. Reddie, Bethany L. Goldblum, Kiran Lakkaraju, Jason Reinhardt, Michael Nacht, and Laura Epifanovskaya. "Next-Generation Wargames: Technology Enables New Research Designs, and More Data." *Science* 362, no. 6421 (2018).
32. Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict."
33. Department of Homeland Security, "Cyber Storm: Exercise Report," 2006.
34. US Naval War College, "Cyber and Innovation Policy Institute Holds 1st War Game with Unique Twist. (November 2018), accessed July 2019. <https://usnwc.edu/News-and-Events/News/Cyber-and-Innovation-Policy-Institute-holds-1st-war-game-with-unique-twist>.
35. Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict."
36. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare and Security Research, Volume 1*, by Julie Ryan (Ed.) (Academic Conferences Limited: 2011).
37. Electron Community, "About Electron" (2019), accessed July 2019. <https://electronjs.org/docs/tutorial/about>.
38. Michael Fischerkeller and Richard Harknett, "Through Persistent Engagement, the U.S. Can Influence 'Agreed Competition,'" *Lawfare*: 2019, accessed October 2019. <https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition>
39. Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it is Important," *Lawfare*: 2018, accessed October 2018, <https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>.
40. James Miller and Neal Pollard, "Persistent Engagement, Agreed Competition, and Deterrence," *Lawfare*: 2019, accessed October 2019, <https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace>.
41. Michael Fischerkeller and Richard Harknett, "A Response on Persistent Engagement and Agreed Competition," *Lawfare*: 2019, accessed October 2019, <https://www.lawfareblog.com/response-persistent-engagement-and-agreed-competition>.

Noisy Operations on the Silent Battlefield

*Preparing for adversary
use of unintrusive
precision cyber weapons*

Forrest Hare | William Diehl

ABSTRACT

Cyber weapons can be divided into intrusive and unintrusive capabilities. Intrusive attacks, which require first gaining privileged access, have earned notoriety in the popular media. However, unintrusive attacks, which can be “noisy” but do not require privileged access, offer a potential cyber adversary many benefits. Using attack methods such as denial of service and telephony denial of service, and energy depletion attacks such as denial of sleep, an adversary can achieve demonstrable effects against a range of targets. These effects can be achieved while reducing the costly burden of pre-attack intelligence-gathering and pre-positioning of exploits that could signal intent or constitute a hostile act. The growth of the Internet of Things in national civilian and defense sectors has resulted in an expanded cyber-attack surface and increased the vulnerability of critical systems to certain unintrusive attacks. In this paper, we define, characterize, and present examples of unintrusive precision cyber weapons used in real-world operations. Given the high likelihood of encountering adversary employment of electronic warfare-like unintrusive capabilities, analyses of cyber conflict and friendly cyber security measures designed to defend against them should be predicated on scenarios that include their employment. Therefore, taking lessons from electronic protection doctrine, we advocate for preparation against the use of unintrusive precision cyber weapons through improved acquisition, training, and integration.

INTRODUCTION

In an insightful article on cyber warfare, “The Ethics of Cyberwarfare,” Dipert divides offensive cyber weapons between those that conduct intrusive attacks, in which weapons gain unauthorized access to the functionality of a targeted system by first achieving privileged access, and unintrusive attacks, in which weapons achieve the desired effects

© 2020 Dr. Forrest Hare, Dr. William Diehl

through cyberspace without having privileged access to the targeted system.^[1] Most research has focused on the challenges, ethics, and other strategic and tactical implications of intrusive attacks. For example, Libicki's analysis of *sub rosa* warfare is predicated explicitly on intrusive attacks, and Herr and Rosenzweig assess export control challenges based on their model of a cyber weapon that contains an exploit used specifically to gain access to a closed system.^[2] However, academia and the popular media have focused less on the use of unintrusive attack methods that have been and could again be employed by adversaries during a conflict. Equally important are the implications of such attacks for the cyber defender responding to them. We argue that in future conflicts, potential adversaries will increasingly employ unintrusive precision cyber weapons (UPCW), which are similar to and facilitated by electronic warfare (EW) capabilities, in that they are both "noisy" and overt. This assertion is premised on several factors, such as the fact that UPCWs require less aggressive and less costly intelligence and can be employed in more diverse situations with a higher level of confidence in their effectiveness than intrusive weapons.

Based on Dipert's classification, we begin with a description of the two classes of offensive cyber capabilities and examples of types of attacks. We then review a selection of previous conflicts where unintrusive cyber weapons were operationally effective and discuss the benefits and challenges of choosing such capabilities over intrusive cyber weapons. Given the high likelihood of encountering adversary employment of UPCWs, potentially integrated with EW capabilities, we further argue that analyses of cyber conflict, and friendly cyber security measures to defend against them, should be predicated on scenarios that include their employment. Based on this assertion, we conclude by recommending where cyber defense measures could be more closely integrated with electronic protect measures.

Intrusive vs. Unintrusive Precision Cyber Weapons

In Dipert's taxonomy, cyber weapons can be divided into intrusive and unintrusive capabilities. Most academic research and popular press reports focus heavily on so-called intrusive cyber attacks, in which an aggressor, be it hobby-hacker, cyber criminal, or nation-state actor, gains some level of privileged access to computer programs, software, or stored data.^[3] Using this class of cyber weapon, the attacker must act from inside the target system; they gain privileged access by using malicious software (malware) to manipulate the target system. Intrusive attacks can be labeled quiet, in that the attackers make a significant effort to remain undetected and leave no noticeable indicators of activity until the payload is activated; the attacker needs another software component or payload to achieve the desired effect against the targeted system during a conflict or contingency. The intrusive cyber weapon might also have a command-and-control entity that could be used to execute the entire operation. However, the attacker might never be able to assess battle damage inflicted on the targeted system, due to a lack of observable external effects.

Cyber-criminal organizations, hacktivists, and purported nation-state actors have conducted well-known intrusive cyber attacks during recent conflicts that required pre-positioned exploits. For example, Russia has been conducting a sustained but undeclared cyber war against Ukraine's military and civilian infrastructure for several years. In December 2015 and again in December 2016, Russia-associated actors attacked Ukraine's financial system, transport, and energy facilities using TeleBots and BlackEnergy malware.^[4] These attacks required privileged access, which Russia gained over the course of six months as malware was downloaded to network systems. The attackers then used network access in energy company computers to pivot to supervisory control and data acquisition (SCADA) devices. When the time came to launch an attack, the actors remotely accessed the control devices and simply shut down the power. In one such event, up to 225,000 people were without power for several hours.^[5]

The attack on the Ukrainian power system began by pre-positioning malware in the targeted systems, which required long-duration cyber reconnaissance that included computer network exploitation (CNE), target development, and network mapping. As we discuss later, such pre-positioned cyber exploits are ephemeral in nature; they can be neutralized, wittingly or unwittingly, by changes in network topology, by rerouting external communication links, or by improved cyber hygiene measures taken by the target organization. Moreover, a presumption of hostility or undeclared aggression either exists or is implied by conducting the cyber exploitation necessary to prepare intrusive attacks on sensitive national systems.

In contrast, an unintrusive precision cyber weapon employs techniques that do not require the attacker to first gain privileged access to achieve an effect on a desired target or to exploit correctable system vulnerabilities. Instead, a targeted device, which could be a node, server, sensor, actuator, or network, is disrupted or degraded so that it cannot function properly for a specific amount of time but is not otherwise permanently damaged; the effects of the attack begin on command and should stop when the attacker stimulus is removed. UPCWs are inherently noisy, in that their application is readily observable to attacker, victim, and third parties. The term "precision" as relates to these weapons refers to both time and space; in other words, the desired effects are achieved against a specific device, with limited collateral impact to non-targeted devices through random self-replication.

Although a potential attacker must understand the general technology of a targeted device, which could require intelligence preparation, research, and engineering capabilities, employing a UPCW requires only limited understanding of the target's specific configuration or of target details that cannot be gained through open sources, such as Internet-facing IP addresses. Moreover, their employment does not require *a priori* insertion of malware or Trojans; rather, the attacks are directed at general properties of the targeted device in conjunction with delivering effects. UPCW capabilities include Denial of Service (DoS) and Distributed Denial of Service (DDoS), Telephony Denial of Service (TDoS), and emerging cyber threats germane to the Internet of Things (IoT), including Denial of Sleep (DoSL).

In DoS and DDoS attacks, the attacker seldom gains privileged access to the target system. They instead often attempt to overwhelm a victim with legitimate or nearly legitimate service requests using normal network communications. DoS and DDoS are remarkably simple but successful attack vehicles, since networked target devices must service client requests in order to function. Typically, no physical or logical damage to target networks occurs; networks are simply denied or degraded for the duration of the attack. One must note, however, that DoS and DDoS attacks are often preceded by a lengthy period of acquiring botnets, which are third-party computing platforms that are maliciously coopted by an attacker, often by intrusive means such as implanting malware. The *a priori* coopting of botnets or other “zombie” devices is not required by an actor with sufficient means to provide its own attacking devices. However, a diverse set of unwitting third-party computing platforms provides topological separation of attack vectors, which makes it more difficult for a defender to use countermeasures (e.g., blocking attacks) while allowing legitimate requests. Cyber preparation of the battlespace to conduct DoS or DDoS is otherwise not difficult, given that most target devices are designed to be easily discoverable and reachable using highly standardized protocols.

In TDoS, an attacker disrupts telephone or associated communication services by initiating an overwhelming number of calls that prevent legitimate users from making calls during the attack; this move can be sustained as long as the attacker wishes to disrupt the targeted phone network. This kind of attack also can be used to support fraudulent activity, for example, by preventing a client from contacting their bank to verify a credit card transaction. Voice over Internet Protocol (VoIP) has made TDoS attacks more dangerous, including those on the legacy public switched telephone network (PSTN). The PSTN was formerly a closed system, is now integrated with IP packets, making attacks easier at the application level. Social media also can be used to initiate mass calling campaigns, as spoofed or anonymous calls are easier to make using these platforms.^[6] As with DoS and DDoS, the intelligence preparations required to employ TDoS are generally not difficult, as many telephone numbers are publicly available, but even where they are not, the easy placement of telephony surveillance devices by cyber criminals and potentially by nation-state actors, such as international mobile subscriber identity catchers, greatly increases the potential for such attacks.^[7]

The onset of new edge-computing enabled through the IoT has greatly expanded cyber-attack surfaces, in particular new attack vectors for unintrusive attacks. Attack surfaces have expanded due to three factors: (1) the sheer number and ubiquity of IoT devices, estimated to reach 24 billion out of 34 billion total Internet-registered devices by 2020; estimates are that 70% will have software vulnerabilities;^[8] (2) low-cost and low-security devices, necessitated by a market model with a very low profit margin;^[9] and (3) new attack vectors that can be used to inject, spread, and direct attacks through non-Internet connections, such as radio frequency, optical, or near field magnetic communication. All of these vectors facilitate attack propagation, even between and among air-gapped systems.^[10]

IoT vulnerability to UPCW attacks was demonstrated during the October 2016 Dyn cyber-attack.^[11] Mirai malware was installed on millions of IoT devices (e.g., web cameras, baby monitors, residential gateways), which overwhelmed the Dyn domain name server with resolution requests and took down large segments of the internet in Europe and North America. Future attacks of this type are increasingly likely to occur with IoT devices, since their low cost and low security standards often result in continued post-purchase use of default credentials.

Another class of UPCW has been made possible by the development and field deployment of IoT devices that often are not connected to electric power sources, relying instead, for example, on AA or 9V batteries. This configuration allows for unintrusive energy depletion attacks that are enabled by attempting to contact target devices using protocols that have varying degrees of legitimacy, which causes them to increase their processing power. Energy depletion attacks can be caused by simple wideband jamming designed to increase the noise environment, and they can cause IoT devices to use more power to transmit.^[12] Attacks of this nature, such as DoSL attacks, can also be more sophisticated.

One well-studied example of a field-deployed IoT device is the wireless sensor network (WSN), which often consists of a simple processing core, such as a microcontroller, and uses a wireless radio standard to transmit environmental or sensor information to a central collector. Most contemporary microcontrollers have a low-power mode, which turns off the central processor and high-frequency clock and then enters sleep mode to preserve battery power during long-term independent operation. In one study, a WSN device was shown to consume up to 400 times more power in receive mode than in sleep mode, and up to 1,000 times more power in transmit mode than sleep mode.^[13] Accordingly, using two standard 3000-mAh AA batteries, it can last 3,300 days in sleep mode but only 5.8 days in receive mode. The study also identified that energy wasted through collisions, control packet overhead, overhearing (i.e., being in receive mode while another node is transmitting), and idle listening (i.e., listening to unnecessary traffic in receive mode) can quickly drain the power of these WSN devices and render them inoperative.

Another type of attack is to target power consumption, which relies on power consumed during authentication. In an age where an adversary could attempt a masquerade, replay, or “man-in-the-middle” attacks, IoT networks need authentication protocols when a new node attempts to join a network through a wired or wireless connection. When devices are in sleep mode, requests to authenticate new devices cause them to enter processing modes, which vastly increases energy consumption.^[14] Energy depletion is exacerbated by the challenges of authentication protocols, whose encrypted data streams can contain thousands of symbols.^[16] To reduce processing and energy resources, IoT devices often use symmetric encryption (i.e., secret key cryptography) for authentication protocols. In symmetric encryption, both parties have the same secret key, which is usually short. For example, the current U.S. Advanced Encryption Standard and commercial encryption innovations such as Google Adiantum use

128-bit secret keys.^[16] However, key distribution is challenging, which is one reason why IoT devices retain their factory settings that usually cannot be changed.

In contrast, in asymmetric encryption (i.e., public key cryptography), keys exist in pairs of public and private keys, and only one entity has the private key of a given public-private pair. Authentication is facilitated by asymmetric encryption, since only a known entity could feasibly respond with the correct private key. Public key cryptography requires orders of magnitude more processing power and much longer public keys (e.g., 256 bits for a current ECC algorithm and 3,072 bits for a current RSA algorithm). Increased use of processing and transmission power results in higher costs for commoditized IoT devices, which in turn results in the industry opting for cheaper but less secure solutions. DoSL attacks enabled by authenticating public key encryption will become more powerful in the next five to ten years, as designers are forced to incorporate post-quantum-resistant public key infrastructure, for which keys could be tenfold longer than current and projected public and private key lengths.^[17]

To summarize, the operational concept of energy depletion attacks, forcing devices to wake repeatedly from sleep mode, to increase processing or transmission power in order to carry out their mission, an adversary need only study IoT network protocols and bombard target networks with traffic that has various degrees of illegitimate or nearly legitimate packets.

Examples of UPCW Usage in Regional Conflicts

The use of UPCW in operational scenarios and as a means to achieve state objectives is not far-fetched; it has been demonstrated on several occasions. In 2007, alleged Russian “patriotic hackers” launched a DDoS attack against Estonia, due to Estonia’s plans to remove World War II monuments honoring the Russians.^[18] These attacks were focused on disrupting government institutions and disabling commerce. The cyber attacks, however, were not followed by or coordinated with kinetic military operations, since aggression against a NATO member was either beyond the limits of Russia’s strategic risk or objectives at the time. The use of non-governmental agents gave the Russian government plausible deniability while successfully sending a message to their much smaller neighbor about how vulnerable it would be in a conventional fight.

By August 2008, the Russians had begun to combine cyber and kinetic operations in their brief conflict with Georgia. Russia conducted DDoS attacks against Georgian internal communications; cyber operations were coordinated with military operations as part of the Russian response to Georgian military operations in the breakaway Georgian regions of Abkhazia and South Ossetia. This was arguably the first coordinated use of military and network-based cyber operations as part of a synchronized strategy.^[19] These attacks were intended to deny, disrupt, and affect the overall flow of information inside Georgia by overloading government sites with requests and disrupting telecommunications nationwide. The attacks did not require exploits to be implanted in advance in the target machines as they used thousands of previously

co-opted zombie bots to send requests. These DDoS also employed structured query language (SQL) injections/cross-site scripting (XSS), which can be used to deny services. Public email addresses were also utilized for psychological operations. These various attacks were ostensibly attributed to Russian “cyber militia” instead of official Russian government.

By 2014, the Russians had honed unintrusive (but noisy and disruptive) cyber operations down to a finely tuned science. They turned to lower technology methods to launch coordinated cyber attacks that disrupted Ukrainian government functions while pro-Russian rebels seized Crimea in March 2014. They simultaneously sowed the seeds of malware exploits for future intrusive cyber operations. The operations against Ukraine consisted of TDoS attacks on mobile phones, which originated in Crimea.^[20] The attackers used equipment installed in the Ukrtelecom networks in the Crimea region under control of Russian forces. However, DDoS attacks on most web services in Crimea were not required by cyber means, as many already were under the physical control of Russian forces by the start of the conflict; in short, the occupying forces simply turned off the servers.

The current and coming increased use of UPCW by Russia in combat scenarios portends closer integration of cyber and EW capabilities, as EW platforms are well-suited to deliver synchronized effects across the multiple attack surfaces utilized by modern IT devices. As a powerful example, Russian cyber operations have been, and are poised to get, much noisier than legacy DoS attacks. Over the last 10 years, they have developed, fielded, and employed battlefield EW capabilities with impunity and are now able to affect cyber conditions at the operational level through integrated platforms. One such example is Russian use of the R-330ZH Zhitel. The R-330ZH conducts barrage noise jamming of tactical radio nets, cell phone emitters, and satellite downlink targets, and it can locally nullify communications and GPS signals. It is designed for detection, analysis, direction-finding and jamming satellite and cellular phone communication systems operated in the frequency from 100 to 2,000 MHz. Effects of the R-330ZH as a battlefield EW system are clearly observable to targeted systems; it is noisy and overt, and the degradation of communications networks ceases when jamming ceases.^[21]

At this point, we have defined and characterized UPCW, discussed the types of attacks where their use might be effective, and reviewed real-world operational scenarios in which UPCW-type weapons were employed. Given this background, we can now discuss the benefits of such weapons to a potential cyber aggressor and why they likely will be employed in future conflicts.

Potential Benefits of Developing and Employing UPCW

The cyber belligerent will enjoy several potential benefits when integrating UPCW with conventional military operations. The first benefit is a reduced need for high-fidelity and difficult-to-gather target intelligence when developing and employing advanced cyber weapons. While an adversary must still invest in research and development against target-specific

capabilities, the *a priori* insertion of fragile malware or Trojans into target networks is not required; rather, the attacks are directed at general properties of the targeted device in conjunction with delivering effects. This benefit can be contrasted with the intelligence requirements for intrusive cyber weapons. Each component of an intrusive cyber weapon system requires specific intelligence; the more complex the capability, the more complex the intelligence required. For example, a capability that employs an intrusion exploit, a remote command-and-control mechanism, the ability to elevate privileges and move laterally in a system without being detected, and a payload to achieve an effect on a specific component within the system requires exquisite intelligence for each component of the weapon. The operator needs to know software versions of the target systems, the target's network addresses, details of the cryptography employed by the defender and of the defenders' operational tactics to avoid being seen by them, and a host of other requirements. Even if the details for building an exquisite cyber weapon can be found on the Internet, the intelligence required to employ the weapon against a specific national security related target network must be gathered by an advanced intelligence organization. What complicates the intelligence requirements further is the fact that the intelligence details will change over time; for example, administrators, network configurations, and software will change. As a result, the intelligence must be constantly checked for accuracy, which requires additional intelligence missions that give the defender repeated chances to be tipped off to malicious activity on their networks.

These enormous intelligence requirements favor countries with advanced signals intelligence (SIGINT) and CNE capabilities.^[22] However, an intelligence organization's ability to support the development of intrusive capabilities does not directly equate with a desire to support their development. Cyber operators will most likely have to compete with national foreign intelligence requirements to satisfy their cyber-development requirements. This would require them to make the case to their intelligence support units that the exquisite cyber weapon's future potential to support military operations outweighs the immediate benefit to leaders from acquiring foreign intelligence. Therefore, there likely would be significant pressure to develop capabilities requiring less detailed intelligence, even in countries with advanced intelligence capabilities. Countries without advanced SIGINT and CNE capabilities would have an incentive to employ UPCW, given that such capabilities would create fewer intelligence-related barriers to entering the cyber conflict. Focusing on UPCW would reduce the need to develop the skill sets and infrastructure required to obtain the highly detailed and perishable intelligence necessary to support employment of intrusive cyber weapons.

A second and directly related advantage is that an unintrusive precision cyber weapon's capability is less ephemeral and requires less technically skilled operators than an intrusive one's. As described by Smeets, cyber weapons are generally more transitory than conventional kinetic weapons because their "ability and effectiveness to cause harm declines relatively quickly."^[23] For example, an offensive cyber capability often can be neutralized before it is used if a network defender upgrades its software or firmware, installs a patch, or changes

passwords. The transitory nature of an intrusive cyber weapon is compounded by the fact that any change made by the defender, whether specifically to increase security or to restructure the domain, could create a formidable barrier to the attacker if they are unaware of the details of the change. A simple measure such as conducting an off-site backup may be sufficient to counter a complex attack. Changes to any component of the target system or its defenses could cause the overall capability of the attack to malfunction and reduce confidence in its ability to achieve effects when and where desired on command. To counteract these factors, would-be aggressors need skilled operators who can develop effective weapons quickly and test their effects against ever-morphing targets. UPCW, on the other hand, can be employed by operators with much less detailed training in their development and employment, as Russia demonstrated in the Georgia conflict.^[24] This increases a military force's ability to train a large cadre of cyber operators, who can train with other combat forces directly in preparation for a conflict. With this consideration in mind, one would expect that, the less complex the cyber weapon, the less transitory it will be, and the greater the likelihood of achieving a return on investment in its development and employment. The potential return on investment would increase whenever the cyber defender further improved its cyber security posture or patched potential vulnerabilities against intrusive weapons.

A third advantage arises from the fact that unintrusive capabilities do not require advance emplacement of exploits that need monitoring, so there is less potential to signal intent before the weapon is employed during a conventional military operation. Even conducting reconnaissance before attempting to emplace an exploit could tip a defender to an attacker's intent if the reconnaissance is sufficiently aggressive. Without the need to maintain access to an exploit that has been inserted in an adversary's cyber system that required privileged access, the UPCW operator can more easily maintain positive command and control of the cyber weapon without any warning signals being broadcast to a target. This increases the chance that the attack can be initiated at the correct location and specified time to support conventional or other cyber operations. The increased precision possible when having direct command and control of the system increases a military commander's confidence in a cyber weapon's ability to support operations as needed. In addition, simplified and direct command and control of an unintrusive weapon should enable the operator to reverse effects more easily and rapidly. On the other hand, when an intrusive weapon is employed for which the attacker expects to lose direct command-and-control ability, the command to cease effects must be encoded in the payload, should that capability be desired. For example, if the "defuze" command is dependent on environmental conditions that could change if the target system software is upgraded, the command may never be delivered.

A related advantage that stems from delivering effects on the outward-facing components of the targeted system is that the cyber operator employing UPCW can measure the effectiveness of weapon employment more directly. When complex cyber weapons are employed that have

effects on targets that are not directly observable—for example, disrupting a server within a closed network—the attacker might never be able to confirm the weapon’s effectiveness. When employing unintrusive measures, the effects on the target are likely more accessible for a battle damage assessment and can be reported to other forces that are relying on the effects of the weapon to conduct their mission. The increased ability to measure the effectiveness of an attack increases both confidence in its use and the probability that a military commander will advocate to integrate the UPCW with conventional military operations.

These advantages cascade to create additional advantages. For example, the increased likelihood of using unintrusive cyber weapons will enable operators to learn from their use and improve their effectiveness. This advantage leads to a greater ability to exercise with the capability and to use UPCW multiple times during a conflict. This increased knowledge and efficacy will increase a commander’s confidence in the future success of UPCW and have a self-promoting influence on their development. It appears, for example, that the Russians have learned from their experiences in Georgia and Ukraine, as we see their military commanders becoming more confident in the effectiveness of UPCW. Gen. Raymond Thomas, former commander of U.S. Special Forces Command, stated that Syria is the “most aggressive EW environment on the planet... They are testing us every day, knocking down our communications.”^[25]

Lastly, there is less pressure to “use it or lose it.” Some authors argue that the transitory nature of intrusive cyber weapon systems increases the likelihood that they will be employed in a preemptive situation because they must be used before they become obsolete.^[26] In fact, if the arguments we have made to this point support the notion that our adversaries are instead developing unintrusive capabilities, which we expect would have less devastating effects on our systems, we also can assume that it reduces the pressure for them to “use them or lose them.” This would possibly reduce the pressure we feel to develop exquisite, intrusive cyber weapons to avoid losing a cyber arms race.

Challenges

Despite the benefits belligerents might gain by using UPCW in a conflict, they also will face challenges. First, noisy cyber weapons can more easily be attributed to an adversary. The noisier the attack, the more quickly the victim will begin tackling the attribution issue. A counterpoint would be that, given that these weapons would most likely be employed during an ongoing conventional military conflict, concern about attribution would most likely not influence the attacker’s decision to employ them.^[27] Even with the potential for attribution, it is difficult to identify the exact origin point of an attack, which creates plausible deniability for specific actors. Moreover, distributed attack surfaces, such as botnets, will obscure the identity of the sponsors of such attacks and increase the potential for plausible deniability.

Second, in any cyber campaign between nation-states, there is a tendency for technically capable, idealistic or nationalistic patriotic hackers to join the fray.^[28] Patriotic hackers traditionally

conduct noisy attacks and do so on purpose, as they want their presence to be felt. They also provide a convenient cover for a military if anonymity is still desired. However, for those who want to act according to the Law of Armed Conflict, the participation of patriotic hackers can lead to a loss of control of cyber actions, as the hackers cannot be controlled as readily as military forces. Therefore, they may not act with the desired precision in terms of the specified target and the duration of the attack. Limited effectiveness in Georgia and indiscriminate attacks on US and Estonian targets during these events caused unwanted problems for Russia.^[29] As discussed by Gelb and Libicki, politicians often fear losing the war less than losing control of the war, therefore, weapons that cannot be controlled effectively by a central command structure are problematic if war is to be a “continuation of politics by other means.”^[30] However, nation-states that are reasonably confident in their ability to maintain control over their populace, including any accompanying internal information campaign, are less likely to be dissuaded by patriotic hackers and may actually exploit this phenomenon to their advantage.

Implications for the Defender

Given the benefits of developing less sophisticated UPCW, the implications for the cyber defender are clear—the defender must prepare for increased adversary use of UPCW, both in future conflicts involving integrated employment of kinetic and non-kinetic weapons, and in periods of heightened tensions where non-kinetic weapons can be used for strategic signaling and psychological effect. Increased cyber security spending in the U.S. Department of Defense, the stand-up of U.S. Cyber Command (USCYBERCOM), and the coordination of improved cyber security with critical infrastructure providers will continue to reduce our vulnerability to cyber weapons in general, and to complex weapons specifically. However, organizations charged with the research, development, and acquisition of cyberspace-dependent systems should clearly understand the vulnerabilities of complex command, control, communications, and intelligence (C3I) and UPCW combat systems, especially those enabled by flexible IoT devices.

Commanders also should consider the increased probability of early use of UPCW and adjust their training and defensive plans accordingly. Given the lessons learned from the employment of UPCW described above, UPCW are likely to be used not only against military C3I and combat systems, but against dual-use systems such as national telecommunications networks and power grids. Such systems support friendly military operations but also guarantee the security and well-being of civilian populations and friendly nations.

Furthermore, while this article takes no position on the merging of cyber and EW operations organizationally, it is clear that EW capabilities have been, are currently, and will be used in the future by potential adversaries to achieve integrated cyber effects. On a related note, the similar effects created by EW weapons and UPCW suggest that cyber defenders may learn from the EW community how to improve cyber defense. For example, Joint Electronic Warfare Doctrine describes the U.S. military’s procedures for conducting frequency-management

functions to ensure availability of the electromagnetic spectrum during a military operation.^[31] Frequency management procedures establish critical requirements for frequency usage and outline coordination requirements with host-nation agencies. Perhaps the cyber defender could implement similar measures to ensure the availability of bandwidth via all mediums, to include RF, during a military operation. An additional electronic protect operation that might translate to defensive measures against UPCW attacks is Electromagnetic Interference (EMI) resolution. EMI resolution is a step-by-step process used to systematically diagnose the source or cause of EMI.^[32] The same procedures could be employed to identify and counter the source of such attacks as TDoS, DDoS, and DoSL.

Finally, while our emphasis is on defense, friendly actors should consider investigating and developing improved UPCW options. This would help them understand the technology and operating characteristics of such weapons and give commanders symmetric response options in case of adversary use of UPCW. A symmetric response may provide options to deescalate a conflict in a manner more predictable than an asymmetric response option. As discussed in the recently published U.S. National Cyber Security Strategy, U.S. forces require response options to meet the mandate to employ military action in response to malicious cyber activities, both kinetic and cyber actions, in order to inflict swift and transparent consequences.^[33] Furthermore, employment of UPCW could meet the USCYBERCOM priority for “persistent engagement” of contesting the adversary below the level of armed conflict.^[34]

CONCLUSIONS

In this article, we have explored the less debated category of cyber weapons called unintrusive precision cyber weapons. We have argued that, although most academic research and sensational press are focused on intrusive cyber weapons that require exploits gained through privileged access, the relative advantages of unintrusive cyber weapons, including the lower bar of entry for a potential belligerent, merit increased consideration. This is especially relevant, given the last decade of increased cyber conflict between nation-state actors and the emergence of new technologies such as the IoT, which have exponentially expanded attack vectors and complicated a defender’s task.

Of pressing concern to the defender are the magnified effects achieved by the integration of cyber and EW capabilities. US research, development, and acquisition organizations should carefully consider the increased attack surface afforded by the IoT and ubiquitous connectivity. The future use of UPCW, including combined cyber-EW attacks, should be studied during training and exercises and envisioned in tactical, operational, and strategic planning. Finally, the US should consider the study, development, test, and evaluation of UPCW capabilities in order to understand the challenges of this domain more fully, and to ensure the continuity of response options across the spectrum of kinetic and non-kinetic conflict. 🛡️

Author Bios

Dr. Forrest Hare

Dr. Forrest Hare is a retired USAF Colonel currently serving as a Solution Architect for SAIC. As a major, he commanded an information warfare detachment in the European Air Operations Center during Operation Enduring Freedom. While assigned to Headquarters Air Force, Dr. Hare was chosen to be on the Chief's Cyberspace Task Force to develop the vision for the Service's operations in its newest warfighting domain. His work contributed to the stand-up of the 24th Air Force and new cyberspace doctrine. After this assignment, he served on the Secretary of Defense staff and was a drafter of DoD Cyber Security policy. Dr. Hare has also served at the National Security Agency and in numerous overseas postings and deployments. In his current position at SAIC, he is developing an ontology-based knowledge model for defense intelligence to improve the integration of cyber threat intelligence with traditional intelligence information.

Dr. William Diehl

Dr. William Diehl is an Assistant Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University (Virginia Tech), a member of the Center for Embedded Systems for Critical Applications (CESCA), and an affiliated faculty member of the Hume Center for National Security and Technology. His area of research is secure and efficient implementations of cryptographic algorithms in hardware and software, including field programmable gate arrays (FPGA), Systems-on-Chip (SoC), microcontrollers, and soft-core microprocessors. Dr. Diehl previously served in the U.S. Navy as a Surface Warfare Officer and Cryptologic Officer, and retired at the rank of Captain. Dr. Diehl completed his B. A. at Duke University, M.S. at the Naval Postgraduate School, Master's Degree in Strategic Studies at the Air War College, and Ph.D. at George Mason University.

NOTES

1. Randall R. Dipert, “The Ethics of Cyberwarfare,” *Journal of Military Ethics* 9, no. 4 (December 2010), 384–410, <https://doi.org/10.1080/15027570.2010.536404>.
2. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007); Trey Herr and Paul Rosenzweig, “Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model,” *Journal of National Security Law and Policy* 8 (2016 2015), 301.
3. See, for example, Libicki, *Conquest in Cyberspace*; Herr and Rosenzweig, “Cyber Weapons and Export Control.”
4. Pavel Polityuk, “Ukraine Points Finger at Russian Security Services in Recent Cyber Attack,” *Reuters*, July 1, 2017, <https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P>.
5. Polityuk, “Ukraine Points Finger.”
6. Rod Wallace, “The Surging Threat of Telephony Denial of Service Attacks,” Industry Report, San Antonio, TX: SecureLogix and Cisco, October 21, 2014.
7. Christopher Krebs, “DHS Response to Senator Ron Wyden,” Letter of Record from Acting Under Secretary, National Protection and Programs Directorate, March 26, 2018, <https://www.documentcloud.org/documents/4429966-DHS-response-to-Wyden-3-26-18.html>.
8. Finjan Team, “IoT DoS Attacks—How Hacked IoT Devices Can Lead to Massive DoS Attacks,” *Finjan Blog* (blog), August 20, 2018, <https://blog.finjan.com/iot-dos-attacks/>.
9. Vladimir Shakhov and Insoo Koo, “Depletion-of-Battery Attack: Specificity, Modelling and Analysis,” *Sensors* 18, no. 6 (June 2018): 1849, <https://doi.org/10.3390/s18061849>.
10. Eyal Ronen et al., “IoT Goes Nuclear: Creating a ZigBee Chain Reaction,” November 21, 2018, <http://www.eyalro.net/project/iotworm/>.
11. Dave Lewis, “The DDoS Attack against Dyn One Year Later,” *Forbes* (blog), October 23, 2017, <https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/>.
12. V. A. Desnitsky, I. V. Kotenko, and N. N. Rudavin, “Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems,” in *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2019, 214–19, <https://doi.org/10.1109/EIConRus.2019.8656795>; Shakhov and Koo, “Depletion-of-Battery Attack.”
13. D. R. Raymond et al., “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” *IEEE Transactions on Vehicular Technology* 58, no. 1 (January 2009): 367–80, <https://doi.org/10.1109/TVT.2008.921621>.
14. C. Gehrmann, M. Tiloca, and R. Höglund, “SMACK: Short Message Authentication Check against Battery Exhaustion in the Internet of Things,” in *12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2015, 274–82, <https://doi.org/10.1109/SAHCN.2015.7338326>.
15. Eduard Marin et al., “On the Feasibility of Cryptography for a Wireless Insulin Pump System,” in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, CODASPY ’16* (New York: ACM, 2016), 113–20, <https://doi.org/10.1145/2857705.2857746>.
16. Paul Crowley and Eric Biggers, “Adiantum: Length-Preserving Encryption for Entry-Level Processors,” *IACR Transactions on Symmetric Cryptology*, December 13, 2018, 39–61, <https://doi.org/10.13154/tosc.v2018.i4.39-61>.
17. Lily Chen et al., “Report on Post-Quantum Cryptography,” Gaithersburg, MD: National Institute of Standards and Technology, April 2016, <https://doi.org/10.6028/NIST.IR.8105>.
18. “A Cyber-Riot,” *Economist*, May 10, 2007.
19. “The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict” (white paper), AFCEA Cyber Committee, May 24, 2012, <https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf>.
20. “Crimea—The Russian Cyber Strategy to Hit Ukraine,” *Infosec Resources* (blog), March 11, 2014, <https://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/>.
21. Rob O’Gorman, “Intelligence Brief: Russia’s Electronic Warfare Capability in Ukraine,” *Open Briefing* (blog), July 7, 2015, <https://www.openbriefing.org/publications/intelligence-briefings/russias-electronic-warfare-capability-in-ukraine/>.
22. Max Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies* 41, nos. 1–2 (February 23, 2018), 6–32, <https://doi.org/10.1080/01402390.2017.1288107>.
23. Smeets, “A Matter of Time.”

NOTES

24. Jeffrey Carr, "Project Grey Goose Phase II Report" (Seattle: Grey Logic, March 20, 2009), ferror.com/pdf/GreyGoose2.pdf.
25. Colin Clark, "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria," *Breaking Defense* (blog), April 24, 2018, <https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/>.
26. Andrew Krepinevich, "Cyber Warfare: A 'Nuclear Option'?" Study on Future Warfare and Concepts, Center for Strategic and Budgetary Assessments, August 24, 2012, <https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option>.
27. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, <https://doi.org/10.1080/01402390.2011.608939>.
28. Forrest B. Hare, "Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?" *Asian Security* 15, no. 2 (May 4, 2019): 93–102, <https://doi.org/10.1080/14799855.2017.1414803>.
29. Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, no. 1 (December 16, 2015), <http://dx.doi.org/10.5038/2378-0789.1.1.1001>.
30. Martin C. Libicki, "Sub Rosa Cyber War," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009); Leslie H. Gelb and Richard K. Betts, *The Irony of Vietnam: The System Worked*, Washington, DC: Brookings Institution Press, 2016; Carl von Clausewitz, *On War*, London: Kegan Paul, Trench, Trübner & Company, 1908.
31. "Joint Publication 3-13.1 Electronic Warfare," Joint Staff, US Department of Defense, February 8, 2012.
32. "Joint Publication 3-13.1."
33. "National Cyber Strategy of the United States of America," Washington, DC: The White House, September 2018, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
34. C. Todd Lopez, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," Government Document, U.S. Department of Defense, May 14, 2019, <https://dod.defense.gov/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/>.

A Quest for Indicators of Security Debt

Simo Huopio

ABSTRACT

Security Debt (SD) manifests itself every day: In the media, we can witness stories about debt defaults: significant data leaks, disruptions of service, and businesses of global companies affected by security incidents. Critical infrastructure customers need more practical tools to ensure that the SD is properly identified in order to make informed risk decisions. Existing tools like security audits and cross-referencing system configuration with available vulnerability information do reveal a lot of data regarding the present state of the system. Many tools that can bring up the hidden security issues like ones included in Secure Development Lifecycles (SDLC) are tuned for the product creation. Some of them can be taken into good use by the customer, but for that, the system should be already procured and in place. In practice, the customer would benefit from a comprehensive and realistic view of the security stance of the system when it is being procured to minimize the nasty surprises the underlying security issues are prone to bring.

This paper reviews the existing approaches used for managing Technical Debt (TD) and continues the discussion about Security Debt. Using this information, a proposal for the Security Debt Indicator Framework (SDIF) was constructed.

Keywords: security debt, technical debt, security tools, SDLC

INTRODUCTION

1.1 Security Debt

Security Debt (SD) is a security domain specific adaptation of well-established Technical Debt (TD), which represents all the work that is left undone in order to gain short term speed and flexibility in product creation. Technical debt concept adoption has been prominent in areas of industry where investments are significant, the systems have an extended lifetime, and modifications and new feature development is common in the middle of the

© 2020 Simo Huopio

system lifecycle: e.g. aviation, maritime, power and utility, and military^[1-3]. In the context of software, TD has been researched mainly regarding what effects it has on the maintainability and the cost of the project. Its effects are apparent: All software projects take some TD but taking an uncontrolled amount of it makes the projects struggle in the end with hard to maintain code and inadequate architecture. There are also numerous examples of catastrophic failures where vast amounts of development work had to be scrapped, and the work had to be started all over again^[4-10].

Security Debt was coined by Chris Wysopal in 2011 and has been further discussed by Dan Geer, and David Conway in the specific context of software^[11,12]. The exemplary white paper by Whitehouse and Vaughn^[13] kept the discussion going^[14]. From these references Security Debt can be defined as all security related work which is not done at an optimal time in order to mitigate all the security issues in the system, known or unknown. The security issues, bugs, and flaws in the system are symptoms of underlying security debt.

Latent, unidentified security issues in the code are transferred to identified security debt with security measures within the development project^[13]. These measures are usually formalized as a Secure Development Life Cycle (SDLC). When the security debt is made visible, risk decisions can be made with the information: Some debt is considered worth fixing, some debt is accepted. So even with SDLC in place and executed properly, there will still be security debt, it will just be visible and in actionable form; not latent and unknown as before.

Whitehouse and Vaughn state that it is common that only the most high-profile security issues are getting fixed, while the low priority issues are left unhandled^[13]. This approach can leave a cumulatively increasing number of lower level issues in the system, which can have a compound effect equal to or greater than a single high severity security bug. Managing this type of security debt is a challenge worth addressing in the new versions of SDLCs.

In the software domain, the security debt has its distinct differences from technical debt: The TD concentrates on the effects, risks, and cost to the manufacturer doing maintenance and further development. The amount of cumulated SD by itself does not add friction or otherwise hinder the system maintainability, but it incorporates significant risk to the business and data of the end user. According to Ernst et al.,^[6,15] the amount of TD is usually quantified as developer work, the amount of work needed to pay back the debt in the code. At the same time, the effects of TD to the actual end product are harder to estimate. On the other hand, the quantity of SD can be hard to estimate as it can hide in a compound of rather small issues. While its effects are easily quantifiable, especially in hindsight: even the smallest security breaches in the news are quoted to cost millions.

While SD is not as easy to quantify as TD, the fact that a large amount of SD is a potentially massive liability to customers makes it an important research subject. Large amounts of TD in the system is also a risk to the customer, but in most cases, TD is more the system vendors

liability. The broader adoption of the Security Debt metaphor could help the security-conscious customers of large and complex software to gather and communicate the security posture of the system in a more comprehensive way.

1.2 Critical Infrastructure customer needs

The viewpoint of this research is of a customer procuring and maintaining a Critical Infrastructure (CI) system. Typical characteristics for such systems are, for example, planning for an extremely long lifecycle (especially by software industry standards), security-conscious and sensitive operating environment, and the unique role of the government entity as a procurer and operator for the finalized system.

The extended lifecycles of such systems will, by itself, mean that system configuration will go through many phases throughout its lifetime: There will be new types of subsystems introduced in a mid-life update after years of the systems first version was taken into use. Some subsystems will face obsolescence and will be replaced with a more modern alternative with some considerable friction. Overall, there will be a technology-security paradigm, and testing technology changes throughout the software industry, which will challenge the fundamental system requirements many times.

Many of the mentioned characteristics can pose extra challenges in defining, onboarding, operating, and maintaining the software integrated into the system. In effect, the maintenance of such a system is more like a research and development project. If the system that has no security issues at the time of procurement is not actively maintained and adapted to the changing environment, the end user is taking a considerable risk that the system will face obsolescence in couple years.

In this context, the concept of Security Debt is very well-suited to communicating the security-related risks of the various aspects of the system in one universal way. As a further development of that notion, it was identified that developing indicators for Security Debt should result in a concrete tool that could directly be taken into use in the help of Critical Infrastructure procurement^[16].

Presently the tools of analyzing and managing the technical debt—let alone the new concept of security debt—are designed to be used in the product creation. The CI customer needs concrete ways to assess the security stance of the system while at the same time having much more limited access to the source code, the underlying things behind the architecture and design choices. The customer communication about such implementation details with the system vendor during the procurement process is limited. Making sure the system requirements are met and that the system onboarding process and the maintenance contract will fulfill the customer needs has enough work without going through the underlying details. Nevertheless, the customer carries the full risk of security issues, while the manufacturer's responsibility is usually very strictly managed.

1.3 Research Question

Breaking down the SD in the CI system end user point of view, we can identify the following distinct areas of SD.

- a) The SD that cumulates in the system during the product creation
- b) The SD that arises from newly discovered bugs in the system during the system lifecycle
- c) The SD that cumulates from system configuration changes during the system lifecycle
- d) The SD that cumulates from the environment and the usage changes during the system lifecycle

Considering the phase of system procurement, the end user needs way to estimate the amount of SD in the system (a), and the ability of the supply chain and the customer to identify and handle the new SD that is created or identified during the system use (b-d). The scope of this research is to create indicators pointing out issues that would prevent end user meeting these needs. The end-user usage of tools and methodologies for analyzing the software binaries or source code, which have been identified as good practice for CI systems in^[16] is left for later research.

From these needs a research question was crafted:

RQ: What kind of indicators could be used to identify the potential for Security Debt in the procurement and maintenance of a Critical Infrastructure system?

2. METHOD

The chosen approach was to use the usage of the SDLC tools and identify best practices for managing SD and security-related TD by the vendor and possible integrators as starting point for constructing the indicators. The researcher used the SDLC standards also as a source for the best practices for the Critical Infrastructure system software maintenance.

This research used a literature study of Technology Debt done for the previous publication, “Thou shalt not fail - Targeting Lifecycle-Long Robustness while being vigilant for the Black Swans”^[16] as a baseline. In addition, a new search was done to widen and update the selection of articles related to the Security Debt, SDLC and security requirements of software project. IEEE Xplore service was used as a primary source for the searches and the papers.

There is a considerable amount of research being done regarding TD in software. Most of it is concentrates on analyzing debt in the light of the work needed on the implementation of future new features, and the software maintenance. Technical Debt is seen as a slowly increasing friction in the software development activities, which must be managed or further development will face serious obstacles. TD is usually measured in units of work time or the equivalent cost, and there is research that strive to validate this measure^[2,4-10,17-21].

In the specific field of technical debt and security, or separately, security debt, there were not many new research papers found. The technical debt-related terms were found to be commonly used by the software engineers when discussing background for security issues^[4]. There was also research regarding mapping different aspects of TD to security issues^[22-26]. Security debt was not usually used as a distinct term, but there were some exceptions. There were numerous news articles stating that security incidents were primarily caused by lax security culture, or badly maintained systems ^[4,7,11,13,14].

A separate search was done to identify the research regarding software security management tools, SDLCs and security requirements. Related standards, models, and requirements tools were identified and familiarized^[27-31].

3. APPLICATION

3.1 *Starting points from the literature*

According to the material, the following tool types were identified as a suitable basis for constructing the identifiers for security debt:

- ◆ Original system requirements: Analysis of the requirements used in system creation related to security: non-functional requirements regarding robustness, integrity and maintenance.^[7,25,26]
- ◆ Secure Software Development Process. SDLC related technical tools, including software composition analysis, threat emulation, robustness testing, and security issue management.^[13,14,32-38]
- ◆ Technical debt management: Tools used in TD estimation that are not included in SDLC tools: Architectural and other source code level complexity analysis, software quality modelling and assessment tools and related standards.^[2,5-7,20]
- ◆ Customer requirements: Analysis of the requirements used in system procurement. In addition to the actual security feature and non-functional requirements, the requirements related to SDLC, security standards, and vulnerability information exchange.^[16]
- ◆ Operations: Analysis of the actions related to the secure operation of the system: configuration, training, usage environment and the usage in conjunction with other systems.^[39]

Using this list as the starting point, a prototype of the Security Debt Indicator Framework (SDIF) was constructed.

3.2 *Indicator design choices*

The SDIF areas were chosen using the tool types discovered from the source material. The use case for the indicators was a very security-conscious customer who was procuring critical

infrastructure system. The data collection was assumed to be done via a dialog with contacts of the system vendor, system integrator and the owner of the to-be-procured system or the customer. The dialog could be implemented as a combination of interview, written questionnaire and document exchange. Should the customer decide so, some of the needed information could be requested through requirements in the procurement process.

The prototype was constructed so that, at the first stage, a rough maturity level was mapped onto each of the SDIF areas with a series of questions. These questions indicate the adoption of best practices as identified by the literature search. At the same time, the availability of further information and data sources was acquired. The result was scored to give a rough top-level indication of how the security debt is handled, which can be useful within the system procurement process.

Table 1: SDIF areas

SDIF Areas	
A	Vendor / Integrator internal system requirements
B	Vendor / Integrator internal software security process
C	Vendor / Integrator internal technical debt management process
D	Customer system requirements and customization
E	Customer capability on the security analysis
F	Customer capability on the secure operation of the system

The questions related to SDIF areas A to C are directed to the system vendor. The same set of questions can be used for an integrator or another third party in a similar role to the system. The questions related to areas D to F are directed for the customer itself. All areas are listed in Table 1.

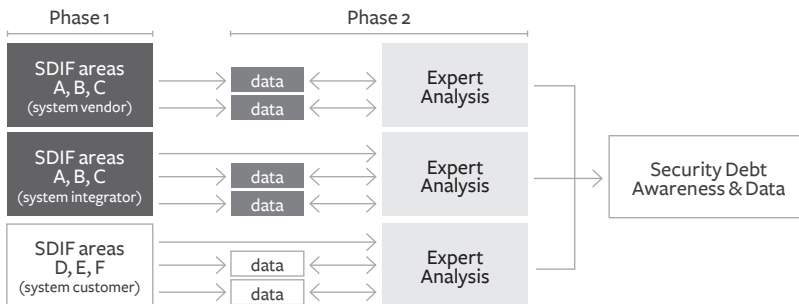


Figure 1: SDIF process

Going through all the areas will give the customer data from multiple dimensions of product creation, maintenance and the planned operation of the system. The process will also give several additional sources of information which can be used to focus on the implementation of a specific area. The overall process is illustrated in Figure 1.

3.3 High-level questionnaire

The prototype SDIF questionnaire is available in Appendix A.

With the first phase of general questions, the customer can get a rough idea of the maturity level of the security debt related choices made in the system. The availability of further data in each SDIF area and the interviewee confidence in the process was also mapped.

3.4 Additional data streams and actions to analyze them

Going through the questions related to each of the high-level SDIF areas will result in additional data streams that will need to be quantified and further analyzed.

It is to be expected that at least some of the data that is requested from the system vendor will be business sensitive, and the vendor may have some reluctance to opening the process. For example, there might be a conscious decision by the vendor to gather TD in the system in order to meet the time to market demands. If the SDIF information is requested in the form of product requirements, this might impact the pricing of the product in order to offset the business risk the vendor is taking in revealing the data.

In some selected areas, the additional data is both straightforward to share and have immediate value. The most evident data streams are listed below with their primary analysis approach. When directly applicable, the related SDIF question (available in Appendix A) is supplied in parenthesis. In other areas, the analysis of the data has to be done via expert opinion analysis.

A: Vendor internal system requirements

- ◆ List of non-functional requirements (A1) to be analyzed to know the case thoroughly.
- ◆ Statistics and trends regarding the test results against the non-functional requirements (A2). This data should show constant testing activity and the stability of the software.
- ◆ Timeline on handling third-party updates (A5) to be analyzed against the customer's own expectations.
- ◆ How long the system will be under active development, and how long the maintenance period will last until it is possibly replaced by succeeding product (A8 & A9)? This data should be analyzed against the customer's own plans on the system life cycle.

B: Vendor internal software security process

- ◆ Analysis of the data that will be sourced from the vendors SDLC implementation (B1 & B7): Threat analysis results and follow-up, risk assessment documentation, security testing results and trends. All critical threats should be mitigated, and the list of accepted security issues (threats, bugs, and misuse) should be acceptable to the customer. This data can also be reused in customer-side threat analysis work.

- ◆ Analysis of BSIMM, or other SDLC maturity metrics data (B3 & B6) should conform intuitively to the customer expectation of the vendor and the product maturity.
- ◆ The used vulnerability feeds followed by the vendor (B8) should include all used 3rd party software components.
- ◆ Data from possible bug bounty programs (B9) should match the data from non-functional requirements testing. The found issues should be properly mitigated.

C: Vendor internal technical debt management process

- ◆ The metrics from the TD management process (C1 & C3) will be cross-correlated with customers own testing and assumptions.
- ◆ The vendor-internal software QA metrics (C2, C4, C5) should show constant operation and overall good software quality.
- ◆ The data available about the vendor's approach to TD can be used in customer-side risk assessment work.

D: Customer system requirements and customization

- ◆ Analysis of the requirements document with all of its detail (D1-D4).
- ◆ Red teaming against the customer customization and configuration of the system (D5-D9).

E: Customer capability on the security analysis

- ◆ On a security sensitive system all of the listed capabilities are considered good practice. Any omissions should be carefully analyzed and written down as accepted risk.

F: Customer capability on the secure operation of the system

- ◆ All mentioned data should be available for further analysis. Any omissions should be carefully analyzed and written down as accepted risk.

3.5 Usage, balancing, and further development

The described process at its present form requires manual work to conduct. It is suggested that in the first phase, the customer go through questions with the vendor in an interview format. This approach gives the opportunity to make quick clarifications regarding the questions and the subsequent data. Gaining access, searching, and packaging the requested additional data in phase two takes time, as does forming expert opinions.

It is evident that, should any of the requested data be set available, the result will be beneficial to the overall security of the system. Applying these indicators before the procurement phase has begun could have the most significant impact on this approach. Then, in the best circumstances, scores from these sections could be used as one parameter in the procurement, even before the system requirements are finalized.

System updates that occur in the middle of its lifecycle can bring significant changes to the system's functionality, usage, and connectivity. These are points where security debt can quickly pile up. Applying SDIF on this phase, even when it has not been applied before, can help the customer avoid potential new security debt. SDIF can give excellent inputs to threat emulation, should the customer also want to apply it at this phase.

The result of this work is a comprehensive starting point for analyzing the critical infrastructure software system in a way that the presence of Security Debt can be indicated and the acts of mitigating it can be started before the related risks are realized.

4. DISCUSSION

4.1 Map and compass on hand

SDIF has been constructed in order to help the customer verify that the best practices in minimizing and handling security debt are in use. The absence or improper use of the tools and approaches mentioned by SDIF is an indicator that the SD is not properly controlled.

The present scope of SDIF cannot be used as a comprehensive indicator of actual SD in the CI software, even though enough data from vendor SDLC process could give some insights. The only way to know the amount of SD is to acquire even deeper knowledge of the software architecture and test results and additionally, to use one's own analysis and testing tools to verify the findings. However, before that can happen, most of the tools and methods mentioned by SDIF must be in use.

Applying the SDIF process will, in any case, increase the customer's knowledge of how the co-operation with the system vendor and possible involved third parties is planned to work should any security incident happen, be it news about new vulnerabilities on the platform the system is built on, or penetration testing results that point a finger at lousy configuration.

We now have a prototype of this framework and we are working to adapt it to internal use. Applying the framework will help the customers be much more knowledgeable in the procurement process, and at the same time, give a positive signal to the companies who have taken secure development seriously. Proper implementation and further development of SDLCs is imperative in order to add the ruggedness needed for the critical infrastructure to survive in the hostile threat landscape.

4.2 Rocky road ahead

Procuring an extensive, critical system already promises a daunting fight through bureaucracy, massive requirements and service level description documents, and a multitude of supplements. Taking on the additional steps to perform an obscure technical risk assessment might be a too much to take on.

Emphasizing the security and technical debt aspects during the procurement process can end up with a hefty price tag. This is a risk especially when the customer implies that the vendor should give out sensitive, internal data that is used in the internal risk assessments.

Still, the assessment of security debt handling cannot be ignored. It would mean too much of blind risk taking. The way forward will be a further development of related standards, reliable maturity models, and other ways to convey the data about the product creation and maintenance process to the customer. Then, it will be easier to trust that the system has been created with due diligence, and the inevitable incidents can be handled in a way that do not lead to catastrophes.

4.3 Quest continues

The next step with SDIF will be testing it with real systems, ones that are already in use and ones that will be procured. It will also be tried in the context of open source software (OSS) onboarding; in this case, the framework might need a variant where the relevant factors can be extracted from the OSS project, the code, documentation and the community itself. An exciting experiment will also be to analyze the data gathered in SDIF using the different security-auditing criteria that are in use on different nations for governmental use. 🛡️

5. ACKNOWLEDGEMENTS

I want to thank my employer for the support for my research and for openness to give my new ideas a chance in the procurement pipeline. The colleagues on my research group at FDRA and Professor Juha Rönning at the University of Oulu also deserve a big thanks for their support and comments.

Author Bio

Simo Huopio

Mr. Simo Huopio is currently working as Research Manager, Cyber Defence, at Finnish Defence Research Agency (FDRA). He received his Master's Degree (CS) from Helsinki University of Technology in 1999 and has since worked in multiple mobile and information security roles in F-Secure and Nokia before joining the Finnish Defence Forces. In addition to his work at FDRA, he is a doctoral student at the University of Oulu. His professional interests include software robustness testing, threat analysis, and practical cyber defence capability development.

NOTES

1. R.G. Muñoz, E. Shehab, M. Weintzke, R. Bence, C. Fowler, S. Tohill, P. Baguley, Key Challenges in Software Application Complexity and Obsolescence Management within Aerospace Industry, *Procedia CIRP* 2015, 37, 24-29.
2. Z. Li, P. Avgeriou, P. Liang, A systematic mapping study on technical debt and its management. *J Syst Software* 2015, 101, 193-220.
3. B. Bartels, U. Ermel, P. Sandborn, M.G. Pecht, *Strategies to the prediction, mitigation and management of product obsolescence*, John Wiley & Sons, 2012.
4. R.L. Nord, Software Vulnerabilities, Defects, and Design Flaws: A Technical Debt Perspective, Fourteenth Annual Acquisition Research Symposium, Naval Postgraduate School, 2017, 67-75.
5. T. Besker, A. Martini, J. Bosch, Impact of Architectural Technical Debt on Daily Software Development Work - A Survey of Software Practitioners, 43rd Euromicro Conference on Software Engineering and Advanced Applications, 2017, 278-287.
6. G. Digkas, M. Lungu, P. Avgeriou, A. Chatzigeorgiou, A. Ampatzoglou, How do developers fix issues and pay back technical debt in the Apache ecosystem? 2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER), IEEE, 2018, 153-163.
7. N.A. Ernst, S. Bellomo, I. Ozkaya, R.L. Nord, I. Gorton, Measure it? manage it? ignore it? software practitioners and technical debt, Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering, ACM, 2015, 50-60.
8. B. Curtis, J. Sappidi, A. Szykarski, Estimating the size, cost, and types of technical debt, Proceedings of the Third International Workshop on Managing Technical Debt, IEEE Press: 2012, 49-53.
9. Z.S. Hossein Abad, R. Karimpour, R.; Ho, J.; Didar-Al-Alam, S.M.; Ruhe, G.; Tse, E.; Barabash, K.; Hargreaves, I. Understanding the impact of technical debt in coding and testing: an exploratory case study, Proceedings of the 3rd International Workshop on Software Engineering Research and Industrial Practice, ACM: 2016; 25-31.
10. R. Marinescu, Assessing technical debt by identifying design flaws in software systems. *IBM Journal of Research and Development* 2012, 56, 9: 13.
11. D. Geer, C. Wysopal, For Good Measure - Security Debt. ;*login*: 2013, 38 no. 4, 62-64.
12. D. Geer, D. Conway, For Good Measure - The Price of Anything Is the Foregone Alternative, *login*: 2013, 38 no. 3, 58-60.
13. Ollie Whitehouse, James Vaughan, Software Security Austerity - Software security debt in modern software development, *Rexx Whitepaper* 2012, 1.
14. Nccgroup blog post: Revisiting security debt: Are we ready to have a discussion yet? Available online: <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/revisiting-security-debt-are-we-ready-to-have-a-discussion-yet/>, accessed on May 1, 2019.
15. A. Ampatzoglou, A. Chatzigeorgiou, P. Avgeriou, The financial aspect of managing technical debt: A systematic literature review. *Information and Software Technology* 2015, 64, 52-73.
16. S. Huopio, Thou shalt not fail - Targeting Lifecycle-Long Robustness while being vigilant for the Black Swans, 23rd IC-CRTS (International Command and Control Research and Technology Symposium), November 6-9, 2018.
17. H. Ghanbari, T. Besker, A. Martini, J. Bosch, Looking for Peace of Mind? Manage your (Technical) Debt: An Exploratory Field Study, ESEM 2017: ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ISBN 978-1-5090-4039-1, IEEE Computer Society Press: 2017.
18. R.L. Nord, I. Ozkaya, P. Kruchten, M. Gonzalez-Rojas, In search of a metric for managing architectural technical debt, 2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture, IEEE: 2012, 91-100.
19. N. Zazworka, C. Izurieta, S. Wong, Y. Cai, C. Seaman, F. Shull, Comparing four approaches for technical debt identification. *Software Quality Journal* 2014, 22, 403-426.
20. A. Martini, T. Besker, J. Bosch, Technical debt tracking: Current state of practice: A survey and multiple case study in 15 large organizations. *Science of Computer Programming* 2018, 163, 42-61.
21. P.N. Bideh, M. Höst, M. Hell, HAVOSS: A Maturity Model for Handling Vulnerabilities in Third Party OSS Components, International Conference on Product-Focused Software Process Improvement, Springer: 2018, 81-97.
22. C. Izurieta, Kimball, D. Rice, T. Valentien, A position study to investigate technical debt associated with security weaknesses, 2018 IEEE/ACM International Conference on Technical Debt (TechDebt), IEEE: 2018, 138-142.

NOTES

23. L. Lavazza, S. Morasca, D. Tosi, Technical debt as an external software attribute, Proceedings of the 2018 International Conference on Technical Debt, ACM: 2018, 21-30.
24. R. Alfayez, C. Chen, P. Behnamghader, K. Srisopha, B. Boehm, An empirical study of technical debt in open-source software systems. In *Disciplinary Convergence in Systems Engineering Research* Springer: 2018, 113-125.
25. M. Benaroch, Managing information technology investment risk: A real options perspective. *J Manage Inf Syst* 2002, 19, 43-84.
26. P. Avgeriou, P. Kruchten, I. Ozkaya, C. Seaman, Managing technical debt in software engineering (dagstuhl seminar 16162), Dagstuhl Reports, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik: 2016.
27. C. Banerjee, S.K. Pandey, Software security rules, SDLC perspective. *arXiv preprint arXiv:0911.0494*, 2009.
28. G. Disterer, ISO/IEC 27000, 27001 and 27002 for information security management, 2013.
29. C. Gikas, A general comparison of fisma, hipaa, iso 27000 and pci-dss standards. *Information Security Journal: A Global Perspective* 2010, 19, 132-141.
30. N.F. Khan, N. Ikram, Security requirements engineering: A systematic mapping (2010-2015), 2016 International Conference on Software Security and Assurance (ICSSA), IEEE: 2016, 31-36.
31. N.M. Mohammed, M. Niazi, M. Alshayeb, S. Mahmood, Exploring software security approaches in software development lifecycle: A systematic mapping study. *Computer Standards & Interfaces* 2017, 50, 107-115.
32. M. Gustafsson, O. Holm, Fuzz testing for design assurance levels, Linköping University, 2017.
33. B. West, M. Wengelin, Effectiveness of fuzz testing high-security applications - A case study of the effectiveness of fuzz-testing applications with high security requirements, KTH Royal Institute of Technology, 2017.
34. S. Ognawala, A. Petrovska, K. Beckers, An Exploratory Survey of Hybrid Testing Techniques Involving Symbolic Execution and Fuzzing, *arXiv preprint arXiv:1712.06843* 2017.
35. Anonymous Application Threat Modeling, <https://www.owasp.org> 2017.
36. J.A. Ingalsbe, L. Kunimatsu, T. Baeten, N.R. Mead, Threat modeling: diving into the deep end. *IEEE Software* 2008, 25.
37. R. Khan, K. McLaughlin, D. Lavery, S. Sezer, STRIDE-based threat modeling for cyber-physical systems, Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES, IEEE: 2017, 1-6.
38. S. Hussain, A. Kamal, S. Ahmad, G. Rasool, S. Iqbal, Threat modelling methodologies: a survey. *Sci.Int. (Lahore)* 2014, 26, 1607-1609.
39. J. Stark, Product Lifecycle Management: 21st Century Paradigm for Product Realisation, In *Product Lifecycle Management (Volume 1)* Springer: 2015, 1-29.

APPENDIX A

A: Vendor internal system requirements

Nr.	Query text	Answer type(s)
A1	Do you have non-functional security requirements? Can you share these requirements and the related process?	Mandatory: Yes/No Optional: Free text & documents
A2	Do you test the product against the non-functional security requirements? Can you share the results?	Mandatory: Yes/No Optional: Free text & documents
A3	Do you have a common security architecture for the security features? What can you share regarding that architecture?	Mandatory: Yes/No Optional: Free text & documents
A4	Do you design and implement security features or functionality in a different manner than other features?	Mandatory: Yes/No Optional: Free text & documents
A5	Describe your software sourcing process: How do you manage requirements, quality, and software releases with third parties?	Mandatory: Free text & documents
A6	What platforms or codebases of the product is shared with your other products? How do you handle possible conflicts between the domains?	Mandatory: Free text & documents
A7	Is the product still in active development?	Mandatory: Yes/No Optional: Free text & documents
A8	How long are you going to support the product actively?	Mandatory: Free text & documents
A9	How long will the security patches be produced? Will their availability be tied to a support contract?	Mandatory: Time, Yes/No Optional: Free text & documents
A10	How confident you are on the completeness of the internal security requirements on scale 1 to 5?	Mandatory: Number Optional: Free text & documents

B: Vendor internal software security process

Nr.	Query text	Answer type(s)
B1	Is there a Secure Development Lifecycle (SDLC) or equivalent in use on R&D? Can you share the process description?	Mandatory: Yes/No Optional: Free text & documents
B2	Are you following a standard like ISO27k? Can you share the details?	Mandatory: Yes/No Optional: Free text & documents
B3	Has the maturity of the company's software security approach been evaluated with BSIMM or equivalent? Can you share the results?	Mandatory: Yes/No Optional: Free text & documents
B4	Do you use robustness testing in product creation?	Mandatory: Yes/No Optional: Free text & documents
B5	How do you plan and schedule the fixing of security issues?	Mandatory: Free text & documents
B6	What security-related metrics do you collect and follow? Are there any metrics data you could share?	Mandatory: Free text & documents
B7	Do you use threat emulation? Can you share the results?	Mandatory: Yes/No Optional: Free text & documents
B8	Are you routinely following the vulnerability feeds of the third-party components included in the product? What feeds do you follow? What is the process to act on findings?	Mandatory: Free text & documents
B9	Do you do additional security testing on the third-party components you use? Have you found issues?	Mandatory: Time, Yes/No Optional: Free text & documents
B10	How confident you are about your software security process (range 1 to 5)?	Mandatory: Number Optional: Free text & documents

APPENDIX A

C: Vendor internal technical debt management process

Nr.	Query text	Answer type(s)
C1	Do you track the technical debt (TD) that is incorporated with the codebase?	Mandatory: Yes/No Optional: Free text & documents
C2	Do you differentiate the TD work with the rest of quality assurance?	Mandatory: Yes/No Optional: Free text & documents
C3	What mechanisms do you use for tracking the TD (for example error ticketing, backlog)?	Mandatory: Free text & documents
C4	Do you routinely use static source code analysis tools for assessing code quality?	Mandatory: Yes/No Optional: Free text & documents
C5	Do you routinely use architectural health analysis tools for assessing potential issues?	Mandatory: Yes/No Optional: Free text & documents
C6	How fast do you apply the new versions of the third-party component code? How do you manage if tooling, architectural or design changes are needed to incorporate the new versions?	Mandatory: Free text & documents
C7	How do you handle software obsolescence, or “code rot”—a situation when the underlying library or other dependency reaches end-of-life, or the needed platform support ends.	Mandatory: Free text & documents
C8	Do you assign TD with financial value (for example “the amount of work needed to fix the issue”)?	Mandatory: Yes/No Optional: Free text & documents
C9	Does your risk management process take TD into account? What other software related risks are incorporated?	Mandatory: Time, Yes/No Optional: Free text & documents
C10	How confident you are on your internal technical debt management process (range 1 to 5)?	Mandatory: Number Optional: Free text & documents

D: Customer system requirements and customization

Nr.	Query text	Answer type(s)
D1	Do you have non-functional security requirements on the system?	Mandatory: Yes/No Optional: Free text & documents
D2	Do you validate the effects of non-functional security requirements?	Mandatory: Yes/No Optional: Free text & documents
D3	Are there software security clauses that state SLA on fixing the issues on the contract?	Mandatory: Yes/No Optional: Free text & documents
D4	Are there requirements to notify, and fix the errors found on third party code included in the system?	Mandatory: Yes/No Optional: Free text & documents
D5	Will there be custom, additional R&D work on the product?	Mandatory: Yes/No Optional: Free text & documents
D6	Will there be any of your own in-house developed code running on the system? Can you share the process of managing this codebase?	Mandatory: Yes/No Optional: Free text & documents
D7	Will the system configuration settings default safely?	Mandatory: Yes/No Optional: Free text & documents
D8	Are there security-related instructions for the configuration?	Mandatory: Free text & documents
D9	Are there a security-related manual or user training available on the system?	Mandatory: Time, Yes/No Optional: Free text & documents
D10	How confident are you that the relevant security issues have been captured in the system requirements (range 1 to 5)?	Mandatory: Number Optional: Free text & documents

APPENDIX A

E: Customer capability on the security analysis

Nr.	Query text	Answer type(s)
E1	Are you able to do your own robustness testing on the product? Can you describe the process?	Mandatory: Yes/No Optional: Free text & documents
E2	Are you able to analyze the results of robustness testing findings? Can you elaborate on the process and resources?	Mandatory: Yes/No Optional: Free text & documents
E3	Do you have access to the product source code? Are you able to analyze and work on it?	Mandatory: Yes/No Optional: Free text & documents
E4	Are you able to send the system vendor technical error reports on any issues found?	Mandatory: Yes/No Optional: Free text & documents
E5	Are you planning to do technical security audits on the system?	Mandatory: Yes/No Optional: Free text & documents
E6	Have you done, or are you planning to do threat emulation, or threat analysis sessions regarding the system? How are you planning to use the results?	Mandatory: Yes/No Optional: Free text & documents
E7	How do you treat new versions of the system software?	Mandatory: Free text & documents
E8	Are you planning to do Software Composition Analysis (SCA) or Bill of Materials (BoM) analysis on the system software?	Mandatory: Yes/No Optional: Free text & documents
E9	Are you following vulnerability databases and able to cross-correlate with the system software composition?	Mandatory: Time, Yes/No Optional: Free text & documents
E10	How confident you are about the capability of doing your own analysis on the product security posture (range 1 to 5)?	Mandatory: Number Optional: Free text & documents

F: Customer capability on the secure operation of the system

Nr.	Query text	Answer type(s)
F1	Are you planning to train the staff who are going to operate the system?	Mandatory: Yes/No Optional: Free text & documents
F2	Does the training include the handling security-related configuration and incident management?	Mandatory: Yes/No Optional: Free text & documents
F3	How do you analyze the effects of the changes in the operating environment of the system (other systems, networks, way of using the system)?	Mandatory: Free text & documents
F4	What kind of usage metrics you are collecting of the use of the system? Is any metric related to security?	Mandatory: Free text & documents
F5	Do you have a Security Operations Centre (SOC) or similar, which will monitor the security status of the system operation?	Mandatory: Yes/No Optional: Free text & documents
F6	How are you planning to decide on, track and manage changes on the configuration of the system?	Mandatory: Free text & documents
F7	How are you going to secure the system physically?	Mandatory: Free text & documents
F8	Are you planning to engage in penetration testing activities to the system?	Mandatory: Yes/No Optional: Free text & documents
F9	How do you plan to decide on the end of life of the system?	Mandatory: Free text & documents
F10	How confident are you that the product is documented, trained, and operated in the way the operation is secure (range 1 to 5)?	Mandatory: Number Optional: Free text & documents

Wargaming and the Education Gap: *Why CyberWar: 2025* Was Created

David Tyler Long

ABSTRACT

Wargames have been an integral part of planning operations since the 19th Century. They are designed to teach and educate players on specific learning objectives using real-life problem sets to advance knowledge and understanding of those problems. With the increased focus on cyberspace operations in the past decade, wargaming is the key to teach cyber-based operations and prepare for the future. *CyberWar: 2025* is an innovative and newly designed interactive wargame that brings together cyber practitioners, policy writers, and decision-makers to gain experience and understanding through iterative gameplay within a virtual environment.

I. INTRODUCTION

The cyber domain has emerged in the past decade, with governments racing to keep pace with twenty-first-century technological changes to remain competitive in an era of potential cyber warfare. What started with William Gibson's short story "Burning Chrome" (1982) and his underground but well-known hit novel *Neuromancer* (1984), the cyberpunk world of hacking and digital espionage has rapidly progressed from science fiction into reality. Gibson's term, "cyberspace," also made the leap from science fiction to describe the new, global, low-intensity fighting domain.^[1] Any government entity, terrorist organization, or even a rogue actor can ping, probe, attack, interrupt, deface, or block digitally stored data on any server or device on an open internet-connected network. Cyber touches just about everything in today's world from economics, logistics, transportation, infrastructure, and communication and information systems. In short, any chip-enabled device that transmits or processes data can be jammed, manipulated, accessed, monitored, and controlled through means of cyber tools and actions.

© 2019 David Tyler Long

The main issue with cyber is not only what it can do or the means of how it can be used, but how fast it is evolving. Cyber is not a singularity, it cannot be contained or locked into place, and it certainly will not allow itself to remain stagnant. Cyber policy in itself should be the same; it should not be a single document that encompasses specific areas of cyber; instead, it should always be evolving to meet the emerging threats in cyberspace. The world has observed how cyber can be used as a means to engage in low-intensity conflicts (in Estonia in 2007 and then in Georgia in 2008, for example) and as a tool for conducting information operations (the 2016 Democratic National Committee cyber-attacks). Nation-state, non-state, and individual entities have widely adapted cyber-attacks through means such as: denial-of-service, malware, man-in-the-middle, spoofing, social engineering, and exploiting. These cyber-attacks have been used as a way to deny, degrade, disrupt, destroy, or manipulate the adversary in cyberspace.^[2]

In recent history, the most common cyber threats have been cyber-crimes, espionage, and intellectual property theft; however, disinformation and malware applications have become more prevalent since 2016.^[3] Current policy and doctrine cannot keep up simply because cyberspace is still widely misunderstood, undefined, and rapidly changing. To advance cyber policy and to successfully defend networks from adversarial cyber-attacks, defense planners should turn to wargaming for inspiration. Because many defense planners are typically removed from cyber operations, wargaming provides them a unique vantage for testing the suitability of any single policy by emulating notional cyber crisis scenarios that they otherwise would not experience. Cyber wargames also have tremendous academic value in education, whether they be used to educate cyber operators, cyber unit commanders and staff, or policy makers.

In 2017 at the Naval Postgraduate School, my research colleague, U.S. Army CPT Chris Mulch, and I designed and developed an interactive web-based cyber wargame called *CyberWar: 2025* to simulate and educate players on cyberspace operations. Our end state for *CyberWar: 2025* was to release a fully functional interactive cyber wargame for use in cyber operations and planning instruction courses. We understood the vital application of wargaming and software-based serious games or games for training (GFT), such as Engagement Skills Trainer (EST), America's Army, and Virtual Battlespace 3 (VBS3), to train and educate the military personnel on specific, mission-required tasks.^[4] Therefore, we adapted these concepts to address the critical gap of cyberspace operations education within the Department of Defense cyber mission. This article aims to fill the gap in cyberspace operations education and understanding. Moreover, in doing so, to ultimately influence cyber policy through insights gained by cyber wargaming.

II. WARGAMING CYBER

Wargaming has been around for centuries, from the earliest introduction of the first board games in the Roman Era, to the introduction of Chess in the Medieval and Renaissance eras, to the evolution of Chess into Kriegsspiel by the Prussians in the 19th Century, to their extensive use of wargames in World War I, and by many others in following conflicts.^[5] The earliest uses

of wargaming involved waging a mock war with moveable game models or pieces on a tabletop map; however, as wargames have evolved into more substantial and complex systems, they often use computers to calculate algorithms and provide an interface for players to advance the game state.^[6] The premise of wargaming is to support problem solving and education by using consistent feedback through shared experiences. A scenario, game end state, game database or recording method, objectives, players, digital or physical models, rules and procedures, and an analytical, post-game review are what generally constitute a wargame. Since the 1970s, military map and model wargames evolved into what are now called serious games.^[7] Commercial and academic sectors adopted this form of gaming for education, training, and operations research purposes. Serious games have become the form of modern wargaming in which games are a means to gain insight and train players while making the training fun and meaningful.^[8] By gamifying the act of waging war, players learn and adapt by, with, and through each other to explore and solve complex situations as well as prepare for the unknown future while maintaining a high level of engagement within the wargame scenario.^[9]

Wargaming has thus become a method for formulating, enacting, and analyzing courses of action to achieve a specific aim, whether military kinetic operations, emergency and disaster relief efforts, or doomsday scenarios. One desired goal of wargaming is associated analysis because it is the means of quantifying the data of wargame outcomes for operational purposes.^[10] The commonality between most map and model wargaming events is that they are dealing mainly with the physical domain. An event that is tactile and physically observable by nature where the rules are clearly defined such as time, resources, locations, distances, and sequence of actions. Wargaming the physical domain is well understood and practiced, but how can we wargame the cyber domain?

To accurately depict the cyber domain, we need to understand what is observable. For example, network traffic is observable with specific tools or equipment. As such, the time, distance, and location between two network traffic points can be determined because of the physics involved. However, because no two routes are the same or are rarely used simultaneously, the time and distance calculations can be asymmetrical. This asymmetry is the result of hardware limitations, software algorithms, and the protocols used in network data transmission. Consider, for example, a bullet fired from a weapon at a target. In the physical domain, the Law of Universal Gravitation and the three Laws of Motion influence the bullet to move in one general direction towards the target.^[11] However, if the bullet misses or does not reach its target, it will eventually impact somewhere or in something along its fired path. This event is observable and can be repeated numerous times with minimal change in the predicted outcome. Conversely, in the cyber domain, there are slightly different rules when it comes to what is observable. For the sake of argument, launching a “cyber bullet,” or an offensive cyber-attack, may or may not hit its intended target.^[2] In reality, the cyber bullet may not hit anything and will cease to exist. This phenomenon stems from several factors, such as Time to Live (TTL), Address Resolution Protocol (ARP), which is heavily documented in the IEEE 802 standards family and RFC 1180

protocol suites that could potentially influence the flow of data packets.^[13] For these reasons, among others, wargaming in the cyber domain is a complicated endeavor, but not impossible.

Generally, wargame design requires deconstructing a problem set down into individual components that are understandable and easy to manage. Wargaming in the cyber domain is no different. Cyber, because of its vast complexity, can be broken down into the significant elements that are aimed at reinforcing the desired learning goals and objectives of the wargame. All other characteristics should be combined or abstracted for simplicity. Establishing a set of rules and game mechanics that mimic the environment as closely as possible is also important. This foundation is the intermediary between the players and the rules. Thus, solid game mechanics, dynamics, and aesthetics (MDA) build the foundation of great wargames. Motivation, goals, player movement, and competition are a few of the mechanical properties, while game state changes, feedback, icons, avatars, and game board pieces making up the dynamics and aesthetics.^[14] As stated in *Interactive Wargaming CyberWar: 2025*, we stated that:

The MDA framework is what builds the bridge between the designer/developer and the player. Strong core mechanics provide the driving force of the game. Dynamics focus on the challenge of the game, such as levels of random events or unpredictability, which assist in creating replay value and provide feedback to the player. Finally, aesthetics are the visual aspects within the game that connect the design value of the game to human emotion and player experiences. The MDA framework easily ties to its lay counterparts in the form of rules, game, and, ultimately, fun. Game mechanics create the rules and form the boundaries of the game. These rules set the scope and challenges that the player must understand, and these challenges are the objectives from which the player learns to gain further experience or knowledge on a subject.^[15]

The MDA framework is the direct psychological connection between the game designer and the player in which each phase of the framework provides and encourages an experience-driven stimulus or behavior.^[16] A major driving factor of *CyberWar: 2025* that involves the MDA framework is the dynamic of player versus player competition. Players become emotionally invested in winning by using the cyber effects at their disposal to outwit and defeat opposing players. This dynamic is the driving force for follow-on game sessions and in indirectly inspiring players to learn and be more successful or daring with their cyber strategy. Relying heavily on the MDA framework to design wargames significantly improves player engagement, therefore increasing the player's understanding and educational value of the wargame.

However, several challenges emerged from exploring how best to develop wargames in the cyber domain. For example, in the physical domain, a map is used to define the attributes of terrain and borders to contain players within a given operational environment. Within the cyber domain, the terrain and borders remain undefined.^[17] Additionally, unlike the physical domain, the cyber domain lacks the real physical obstacles that are readily accessible to the game's designers. Avatars, game board pieces, player movement, and competition has to be built and

defined. Specific learning cyber objectives have to be clear, concise, and well established to support the mechanics and dynamics of the MDA framework. These learning objectives must tie to current cyber policy while at the same time, adapt to emerging threats and best cyber practices in order to maintain validity and realism within the cyberspace operations field of study. There also needs to be unstated and non-explicit mechanics to address the risk probability of cyberspace operations, referring back to the “cyber bullet” example, which takes into account dynamic actions within a rapidly changing environment.^[18] Realism, complexity, and high replay value are also vital in all wargaming sessions. The end goal is to keep players engaged during a game and learning through repetition, mistakes, and consecutive games^[19]. Finally, we wanted to create a game that could assist defense planners in developing cyber policies that would have wide-use application for multiple organizations and entities without being constrained for DoD use only. It is with these design challenges in mind that we created *CyberWar: 2025*.

III. THE GENESIS OF CYBERWAR: 2025

In the field of cyber wargaming, there were few options available before the creation of *CyberWar:2025*; most cyber-based wargames were marketed for business and industry.^[20] Although revolutionary, these wargames were limited to cybersecurity, incident response, and recovery from a cyber-attack. *CyberWar: 2025* is unique in its ability to allow players to experience a multifaceted attack-and-defend scenario in a simulated cyberspace environment. The overall objective of *CyberWar: 2025* is to accrue as much territory as possible from competing players by accessing and maintaining control of key server nodes and networks, defending your network from these adversaries, and ultimately knocking out adversaries from the game by denying or destroying critical server nodes in their network. Victory implies that players develop and execute a sound cyber strategy using defensive, offensive, or exploitative cyber effects. *CyberWar: 2025* thus gamifies the cyber realm by abstracting and combining the cyber specific minutia of network protocols, devices, and tools into a simplified view and design of cyber-effects, server nodes, network links, and player bases. Designed and developed at the Naval Postgraduate School in 2017, *CyberWar: 2025* began as an innovative wargame concept that underwent four key evolutions before becoming the educational solution that it is now.

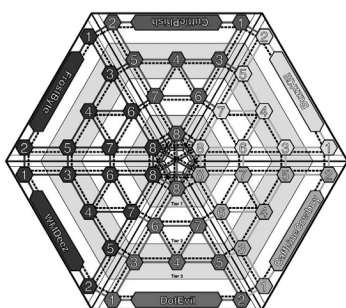


Figure 1. Development View of *CyberWar:2025*

The first evolution of *CyberWar: 2025* took shape in the design of a single large hexagonal game board, composed of six player bases divided into six equal domains, with each holding forty-eight small interconnecting server nodes. Each tier, ranging from one to four, represented the additional cost incurred by the player when executing cyber effects on a tier outside the player's domain. This tiered approach restricts the player's operational movement to the center of the board while signifying that each server node is a control point. The separate domains denoted that other players were operating as unknown actors within the cyberspace domain, each vying for control of the server nodes. Removing player-specific roles such as state or non-state actors allowed players to experiment with their cyber strategy in an equal playing environment devoid of specific game traits or unique player characteristics. During this evolution, cyber effects, costs, and adjudication rules were tested and refined.

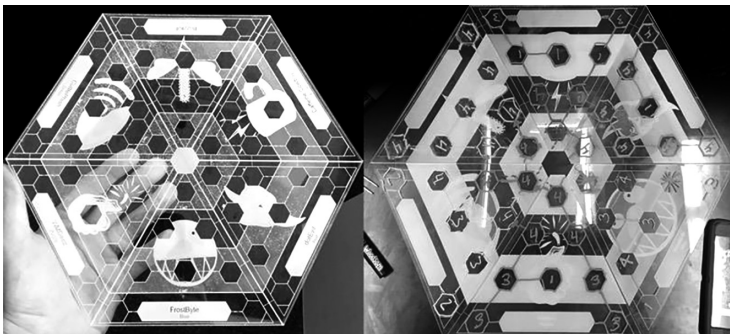


Figure 2. Both Player and Observer Table-Top Boards

The second evolution proved simple enough to play as a tabletop game. This version used six small laser-etched acrylic boards for the players, with a larger six-piece board for the observers and adjudicators. Players were tasked with developing offensive and defensive cyber strategies to disarm or defeat opponents using any of the combined nine cyber effects in the game. Cyber effects available to each player for Defensive Cyber Operations (DCO) or Computer Network Defense (CND) included: Secure, Expel, and Analyze. Overt cyber effects for Offensive Cyberspace Operations (OCO) or Computer Network Attack (CNA) included: Acquire, Manipulate, and Deny. Finally, covert cyber effects for Computer Network Exploitation (CNE) included: Scan, Exploit, and Implant. Each cyber effect had an associated cost, depending on which and where the effect was used. Decisions were written down on acrylic boards using chalk ink markers. Boards were then collected and the game director calculated the results to determine who was winning and losing territory and ultimately the wargame. Consequently, a looming drawback to this approach that emerged was the timing factor. The game mechanics limited course of action selection for six people to approximately twelve rounds, which took about two hours to play, given deliberations. This constraint called for a more efficient solution.

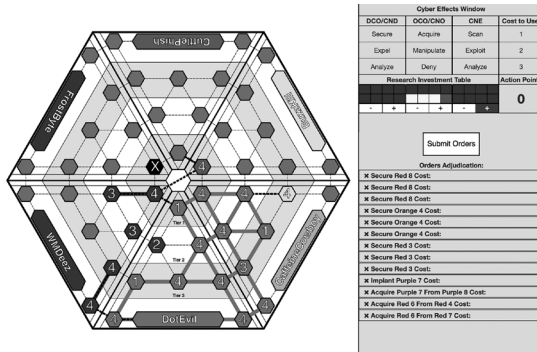


Figure 3. *CyberWar: 2025* Beta Version

The third evolution aimed to reconstruct an interactive and playable beta version of *CyberWar: 2025* in a software environment for responsive game state feedback. In nine months, the computer version of *CyberWar: 2025* was developed entirely from scratch using JavaScript code in order to support cross-platform play with commonly used web browsers such as Firefox, Chrome, and Safari. This improved *CyberWar: 2025*'s efficiency as it became possible to play over forty rounds in a game session within an hour; however, game sessions were limited to time or rounds because the endgame of domination and a few other plugins were not fully developed. The goal of this evolution was to conduct rigorous tests and evaluations through live trial-and-error game sessions. These game demonstrations proved valuable as they provided a platform to track and collect any issues, MDA or otherwise, and garner player reactions and feedback from the game. While the feedback was extremely positive, *CyberWar: 2025* needed several more changes to become a fully functional and interactive wargame.

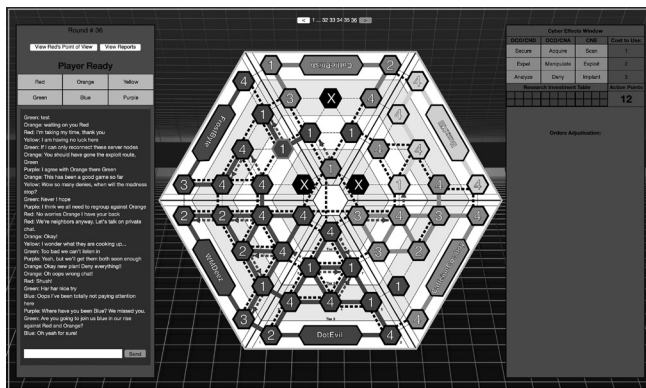


Figure 4. *CyberWar: 2025* Version 1.1 Board from Dot Evil's View

The fourth evolution, or the version 1.1 release of *CyberWar: 2025* focused on the implementation of private and public chat to facilitate in-game communication, enable alliances, and provide the ability for players to conduct information operations against others. Other features

included a single endgame scenario, end-of-round reports, game history, minor aesthetic game board changes, a player ready indicator, and an unrestricted observer view. The majority of these changes were issues that were addressed as player feedback during prior beta testing sessions. The final result of this development evolution is to install *CyberWar: 2025* onto the Naval Postgraduate School’s GlobalECCO server and open the wargame up to public play over the open internet.^[21]

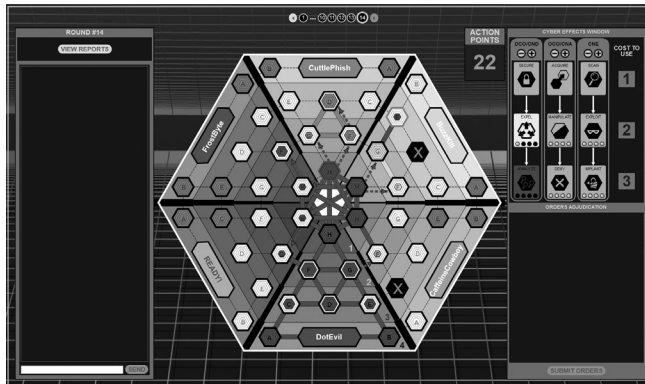


Figure 5. *CyberWar: 2025* Version 1.2 Board Redesign

The NPS GlobalECCO team updated the visuals of *CyberWar: 2025* to make the board view more aesthetically engaging, appealing, and accessible for players by using simplified icons, clearer colors, and icon-based round reports. Version 1.2, the final design for *CyberWar: 2025*, is available for public use on Global ECCO once users have created an account

IV. THE MECHANICS OF CYBERWAR: 2025

CyberWar: 2025 sets itself apart from traditional wargaming because players interact with the game through a web browser which provides efficient, timely, and accurate orders adjudication, thus eliminating the factor of human error in calculating results. Using their mouse to click on server nodes adjacent to those the player has already acquired and linked to their base, the browser shows a drop-down actions menu of potential actions from which the player can choose. Upon selecting and confirming these actions, the player’s orders are stored in an adjudication queue until the player submits their orders to the server. Each player has a private client view, separate from another player’s view, so players cannot interfere with another player’s actions or see what other players are doing between each round. After each player has submitted their orders, the client view transmits these actions to the server for adjudication and the game state is updated to reflect the player’s results.

CyberWar: 2025 also uses consecutive rounds to denote the passage of time within a game session. While time is not proportional to reality (e.g., one round equals a year), when players take actions or put investments to unlock additional cyber effects, these actions and cyber

effects do not become available until the following round. Resources, in the form of Action Points, represent the currency in which a player has to accumulate and manage throughout the entirety of a game session. Action Points are acquired through gaining and holding territory by accessing the server nodes on the board, either overtly or covertly. After each round successfully adjudicates, the number of positively linked server nodes to that player's base are tallied; that amount is the number of Action Points a player can spend to enact their cyber strategy. These Action Points are for further investment into the remaining six cyber effects or to be used as the cost necessary to launch these cyber effects against other players. Players are recommended to use all their Action Points since they do not carry-over for future rounds.

In the beta version of *CyberWar: 2025*, games were limited to time and rounds played and the player with the most Action Points at the end was deemed the winner; however, with the release of version 1.1, endgames were implemented. The only endgame option currently available is domination. In domination, players fight to hold on to their server nodes and maintain network links. The loss of too many critical server nodes and network links will remove the player from the game, with the player remaining claiming victory.

V. HOW ACTIONS IN CYBERWAR: 2025 RELATE TO THE OPERATIONAL ENVIRONMENT

Several underlying game mechanics within *CyberWar: 2025* directly simulate real-world effects and events that have been observed in the cyberspace operational environment. The cyber effects of Secure, Acquire, Analyze, Expel, and Scan are straightforward in their correlation between the modeled game environment and the real world. The only slight difference is with the Secure cyber effect. The association of the Secure cyber effect to reality is with the standard practice of hardening servers and other devices on a computer network. The additional mechanic of increasing the sever node value that does not relate is the mathematical probability involved in launching a cyber effect and its success rate. Having a stronger or better computer in cyber does not mean that there is a higher chance of success in a cyberspace operation.

In Department of Defense Joint Publication 3-12, Manipulate is a cyber-attack which “controls or changes information, information systems, and/or networks” for denial or misinformation effects on the intended target.^[22] When players use the Manipulate cyber effect, they are by definition launching a spoofing network attack and misattributing their action as another player. However, the attacker can also mask their overt action as their victim, which emphasizes the common practice of “hiding in plain sight.” The victim of the attack will think, however, that the attack is coming from another player of whomever the attacking player's manipulate effect identifies. The reasoning behind this cyber effect is to show that cyberspace operations do overlap into the information operations realm. When a defending player notices that an adversary has acquired one of their server nodes within their domain, the typical reaction is to retaliate or acquire that server node immediately. However, if the defending player executes

Scan or Analyze, the attacking player will be correctly identified, and the following actions are solely up to the cyber strategy of the defending player.

Implant is a dual-use cyber effect. Firstly, it modifies the other actions of Acquire, Exploit, Manipulate, and Deny by improving the attacker's odds of success during adjudication. For example, when an attacking player's server node is at the maximum value, and the defending player's server node is the same, Implant reduces the defending player's server node to its minimum for that round, thus increasing the odds of success. *CyberWar: 2025's* Implant effect is a combination of disrupt and degrade in the JP 3-12, because of its dual use as a modifier for offensive and exploitation cyber effects in-game. Implant by itself is always a success just like Scan, Analyze, and Secure; however, the follow-on actions may not always succeed. Secondly, when Implant is used on an adversary's base and is successful, the defending player is temporarily locked out from play for one round in the following turn. This secondary use of Implant is closely related to the ransomware attacks like WannaCry and NotPetya, although players cannot pay out Action Points to revive their network, which is a specific requirement in ransomware.^[23] Implant is a straightforward vulnerability cyber effect and similar to its real-life counterparts; however, Implant is over-simplified to reduce the *CyberWar: 2025's* overall complexity and game mechanics.

The Deny cyber effect is directly tied to the Deny and Destroy definitions within the JP 3-12 of Cyberspace Operations.^[24] Within *CyberWar: 2025*, Deny is the "nuclear option" of permanently removing a server node from the game board. The only difference between Deny in the game versus reality is that in most cases when a server or a device is destroyed in the real-world, it can be replaced or rebuilt; *CyberWar: 2025* does not have this mechanic developed as of the version 1.1 release.

There are also a couple of side mechanics that have a direct relationship within the cyberspace operational environment. The most important one is the idea of blockchain by creating a network of networks within the game. In *CyberWar: 2025*, it is essential to understand the practical application of redundant network paths. When a player has a vast server node network, and a critical server node is denied, that player's entire cyber strategy is drastically less effective. That is until the player regains the lost server node or rebuilds an alternate path, both of which require time, resources, and luck. Another important side-mechanic is the methodology of exploitation. Using Exploit in *CyberWar: 2025* allows an attacking player to gain access to an adversary's server node covertly. However, there can be multiple exploited players on any one server node at a time, which is the exact opposite of the Acquire cyber effect, which only allows one player overt control of a server node. Exploited server nodes are not advertised to the defending player. The only way to identify and remove covert players from their network is to Scan or Analyze and then execute an Expel cyber effect on that specific server node. In the JP 3-12 (R) dated 05 February 2013, exploitation was not explicitly addressed in terms of pertinent it is to the cyber mission. However, in the June 2018 publication of the JP 3-12,

exploitation covers topics of target access: intelligence, surveillance, reconnaissance, command, control, and enabling offensive capabilities.^[25] Exploitation is vital to cyberspace operations because it drives the intelligence cycle and enables follow-on actions. Exploitation is represented in *CyberWar: 2025* by allowing players to operate well within an adversary's domain and execute cyber effects without having to be overtly identifiable.

VI. FILLING THE CYBER EDUCATIONAL GAP THROUGH EXPERIENCE

CyberWar: 2025 was designed to be played iteratively and supported through feedback during instructor-led sessions. It is a means to simulate abstracted and high-level cyberspace operations in an engaging and responsive learning environment. The underlying mechanics do not exclusively teach cyber or cyberspace operations; however, *CyberWar: 2025* opens up the room for discussion between both seasoned cyber practitioners and those who are new or have little to no experience with or understanding of cyber-based operations. Through open dialogue in post-game sessions, players discuss their envisioned cyber strategy and describe their experiences and whether their strategy was successful or not. During live sessions, players are open to asking questions on how specific cyber effects work and the conditions in which to use them; this happens when players are first introduced to the game and its interface. For example, in the initial stage of a new game session, players have unlocked for them the primary cyber effects of Secure, Acquire, and Scan to execute their strategy. Limiting the players to these effects early on keeps players focused on the essential tasks of seek, attack, and defend. However, as players progress and acquire more server nodes, they are able to unlock the additional cyber effects, if they choose to do so. This phase of the game is where the questions on *CyberWar: 2025's* mechanics begin. When players discuss their actions openly, at least for players who are learning the game for the first time, they understand the game better and can adapt to the mechanics of *CyberWar: 2025* quickly.

As a game session progresses through round after round, players will find that the network map ebbs and flows in control based on the multiple actions from each player. *CyberWar: 2025* is designed so that each consecutive round in a single game session provides new challenges for a player overcome. For example, a player who has held a defensive strategy so far may find that in the next round, several players have infiltrated their network. Therefore, they are forced to counter-attack and regain the server nodes in their domain. Another example is when the playable game board is drastically reduced or when players' network is diminished in size because of a successful adjudication from a deny cyber effect. From this point on, players are forced to work around or adopt a new cyber strategy because of the condensed amount of available server nodes left on the board. The dynamic changes that can occur are all viable teaching points that an instructor will explain in the post-game analysis of a session.

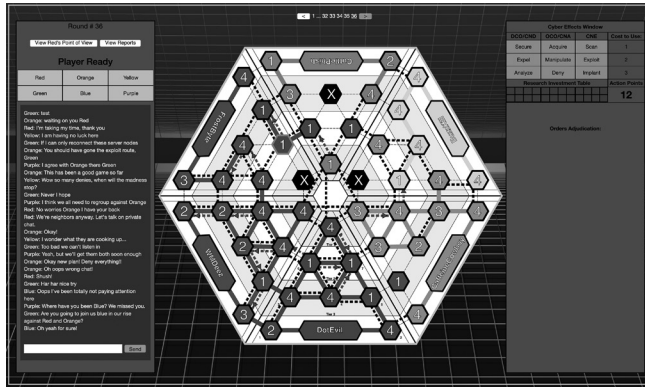


Figure 6. *CyberWar: 2025* Version 1.1 Board Entire Observer View

When a game session concludes, the instructor can reopen the discussions using the observer view of the game board. Going back in time using the history tab embedded in the client game view, the instructor can replay the game round by round, conversing with players directly on their cyber strategies, desired expectations, and outcomes. At the same time, the adversarial players can comment on how their actions may have impacted the initial player’s strategy. After the game review is complete, players are recommended to replay the *CyberWar: 2025* a second time and encouraged to adopt a different cyber strategy to see if their outcomes change.

The significant benefit in *CyberWar: 2025* is that every game is unique because of the underlying adjudication mechanics and various player actions. With each new game session, players will rarely have the same experience in successive games. Through playing iterative game sessions, players learn by gaining experience through trial and error. During the beta testing phase of *CyberWar: 2025*, there were over 25 live player demonstrations, each averaging four hours in length per session. The structure of each demonstration was a quick initial block of instruction on the game and then a quick “hands-on” play session. Immediately afterward, *CyberWar: 2025* was played for approximately an hour and a half with a 30-minute post-game review. Finally, the game was played again for another hour and a half with another 30-minute game review. Players consistently noted that they felt more comfortable with the game during the second play session, and most players adopted a cyber strategy vastly different from their first playthrough. It is also crucial to note that players interacted with each other and the game director during the post-game review discussions. When the *CyberWar: 2025* demonstration concluded, players and observers felt more comfortable with and knowledgeable about cyber-space operations.

CONCLUSION

Wargaming is an integral part of planning and execution of operations and it has influenced policy and doctrine across all services of the military and government. The practical application of wargaming is limitless with new ideas and innovations being tested every year. We have conducted wargames for land, sea, and air warfare; cyberspace should be no different. *CyberWar:2025* is that means for wargaming cyberspace operations, and it is a starting point for future cyber wargames. 🛡️

Author Bio

David Tyler Long

United States Army Master Sergeant David “Ty” Long is a field operations and cyber researcher for a Department of Defense testing and evaluation center at Kirtland Air Force Base, Albuquerque, NM. He is the creator and developer of *CyberWar: 2025*, which was the direct result of the research work that he and co-writer, Major Chis Mulch, completed during their Master’s studies in Political Warfare and Information Strategy at the Defense Analysis Department, Naval Postgraduate School. Their thesis, titled “Interactive Wargaming *CyberWar: 2025*,” described the vital need for cyber wargaming and the development of *CyberWar: 2025*. Master Sergeant David Long is also a senior software engineer and formerly cyber-warfare and information operations practitioner for the United States Department of Defense.

NOTES

1. William Gibson, *Burning Chrome*, Reprint edition (New York: Harper Voyager, 2003); William Gibson, *Neuromancer* (New York: Ace Books, 1984).
2. Department of Defense, “Joint Publication 3-12 Cyberspace Operations” (Department of Defense, June 8, 2018), II–7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.
3. Misha Glenny and Camino Kavanagh, “800 Titles but No Policy—Thoughts on Cyber Warfare,” *American Foreign Policy Interests* 34, no. 6 (November 1, 2012): 287, doi:10.1080/10803920.2012.742410; Carl Bildt et al., “The Arms Race in Cyberspace,” *Project Syndicate*, November 17, 2017, <https://www.project-syndicate.org/bigpicture/the-arms-race-in-cyberspace>.
4. United States Army, “Engagement Skills Trainer (EST),” USAASC, December 21, 2015, <http://asc.army.mil/web/portfolio-item/engagement-skills-trainer-est/>; United States Army, *America’s Army*, Windows (United States Army, 2002), <https://www.americasarmy.com/>; Susan G. Straus et al., “Collective Simulation-Based Training in the U.S. Army: User Interface Fidelity, Costs, and Training Effectiveness” (Santa Monica, CA: RAND Corporation, n.d.), 1–3, https://www.rand.org/pubs/research_reports/RR2250.html; Christopher Herr and Dennis M. Allen, “Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors,” *Software Engineering Institute*, July 2015, 5, doi:10.1145/2751957.2751958.
5. Roger C. Mason, “Wargaming: Its History and Future,” *The International Journal of Intelligence, Security, and Public Affairs* 20, no. 2 (May 4, 2018): 77–83, doi:10.1080/23800992.2018.1484238.
6. David Tyler Long and Christopher M. Mulch, “Interactive Wargaming CyberWar: 2025” (Naval Postgraduate School, 2017), II, Calhoun, <http://hdl.handle.net/10945/56758>; Mason, “Wargaming: Its History and Future,” 88.
7. Mason, “Wargaming: Its History and Future,” 91.
8. Torsten Reiners and Lincoln C. Wood, eds., *Gamification in Education and Business* (Cham: Springer International Publishing, 2015), 4, doi:10.1007/978-3-319-10208-5.
9. Peter Perla and Ed McGrady, “Why Wargaming Works,” *Naval War College Review* 64, no. 3 (January 2011): 2.
10. Peter P. Perla, “War Games, Analyses, and Exercises,” *Naval War College Review* 40, no. 2 (1987): 1, <https://digital-commons.usnwc.edu/nwc-review/vol40/iss2/7>.
11. “Law of Gravity,” accessed July 25, 2019, <https://physics.weber.edu/amiri/physics1010online/WSUonline12w/OnLine-CourseMovies/CircularMotion&Gravity/reviewofgravity/ReviewofGravity.html>; “Newton’s Three Laws of Motion,” accessed July 25, 2019, <https://www.pas.rochester.edu/~blackman/ast104/newton3laws16.html>.
12. Department of Defense, “Joint Publication 3-12 Cyberspace Operations,” II–7.
13. “LMSC, LAN/MAN Standards Committee (Project 802),” accessed July 25, 2019, <http://www.ieee802.org/>; C. J. Kale and T. J. Socolofsky, “TCP/IP Tutorial,” accessed July 25, 2019, <https://tools.ietf.org/html/rfc1180>.
14. Robin Hunnicke, Marc Leblanc, and Robert Zubek, “MDA: A Formal Approach to Game Design and Game Research,” *Press*, In Proceedings of the Challenges in Games AI Workshop, Nineteenth National Conference of Artificial Intelligence, 2004, 5.
15. Long and Mulch, “Interactive Wargaming CyberWar: 2025,” 26–27.
16. Hunnicke, Leblanc, and Zubek, “MDA: A Formal Approach to Game Design and Game Research,” 2.
17. Department of Defense, “Joint Publication 3-12 Cyberspace Operations,” I–12.
18. “Learning Cyber Operations Through Gaming: An Overview of Current and up and Coming Gamified Learning Environments | CSIAC,” accessed July 25, 2019, <https://www.csiac.org/journal-article/learning-cyber-operations-through-gaming-an-overview-of-current-and-up-and-coming-gamified-learning-environments/>.
19. Herr and Allen, “Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors,” 7.
20. Tucker Bailey, James Kaplan, and Allen Weinberg, “Playing War Games to Prepare for a Cyberattack,” *McKinsey Digital*, July 2012, <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack>.
21. “Home - GlobalECCO,” accessed July 26, 2019, <https://globalecco.org/>.
22. Department of Defense, “Joint Publication 3-12 Cyberspace Operations,” II–7.
23. Josh Fruhlinger, “The 6 Biggest Ransomware Attacks of the Last 5 Years,” *CSO Online*, April 5, 2019, <https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html>.
24. Department of Defense, “Joint Publication 3-12 Cyberspace Operations,” II–7.
25. *Ibid.*, IV–9, IV–8, II–1.


THE CYBER DEFENSE REVIEW


CONTINUE THE CONVERSATION ONLINE

 CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

 Facebook [@ArmyCyberInstitute](https://www.facebook.com/ArmyCyberInstitute)

 LinkedIn [@LinkedInGroup](https://www.linkedin.com/company/ArmyCyberInstitute)

 Twitter [@ArmyCyberInst](https://twitter.com/ArmyCyberInst)
[@CyberDefReview](https://twitter.com/CyberDefReview)



ARMY CYBER INSTITUTE ♦ WEST POINT



THE ARMY CYBER INSTITUTE IS A NATIONAL RESOURCE FOR RESEARCH, ADVICE AND EDUCATION IN THE CYBER DOMAIN, ENGAGING ARMY, GOVERNMENT, ACADEMIC AND INDUSTRIAL CYBER COMMUNITIES TO BUILD INTELLECTUAL CAPITAL AND EXPAND THE KNOWLEDGE BASE FOR THE PURPOSE OF ENABLING EFFECTIVE ARMY CYBER DEFENSE AND CYBER OPERATIONS.