

THE CYBER DEFENSE REVIEW

Operationalizing the Information Environment:
Lessons Learned from Cyber Integration in the USCENTCOM AOR

General Joseph L. Votel

Major General David J. Julazadeh

Major Weilun Lin



Intelligent Autonomous Agents are Key to
Cyber Defense of the Future Army Networks

Dr. Alexander Kott

Disinformation -
Дезинформация (Dezinformatsiya)

Aristedes Mahairas
Mikhail Dvilyanski

The Future of Cyber Defense...
Going on the Offensive

Angela Messer
Brad Medairy

Culture in a Murky World:
Hijab Trends in Jihadi Popular Culture

Elizabeth Oren

Cultivating Technology Innovation
for Cyberspace Operations

Colonel Stoney Trent

INTRODUCTION

The Cyber Defense Review:
Cyber Conflict in a Competitive World

Colonel Andrew O. Hall

BOOK REVIEW

On Cyber: Towards an Operational Art for Cyber Conflict
by Gregory Conti and David Raymond

Dr. Jan Kallberg

THE CYBER DEFENSE REVIEW

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

Dr. Harold J. Arata III
(Cybersecurity Strategy)

Prof. Robert Barnsby, J.D.
(Cyber & International Humanitarian Law)

Maj. Nathaniel D. Bastian, Ph.D.
(Advanced Analytics/Data Science)

Dr. Aaron F. Brantly
(Policy Analysis/International Relations)

Dr. Chris Bronk
(National Security)

Dr. Dawn Dunkerley Goss
(Cybersecurity Optimization/Operationalization)

Dr. David Gioe
(History/Intelligence Community)

Col. Paul Goethals, Ph.D.
(Operations Research/Military Strategy)

Dr. Michael Grimaila
(Systems Engineering/Information Assurance)

Dr. Steve Henderson
(Data Mining/Machine Learning)

Ms. Elsa Kania
(Indo-Pacific Security/Emerging Technologies)

Maj. Charlie Lewis
(Military Operations/Training/Doctrine)

Dr. Fernando Maymi
(Cyber Curricula/Autonomous Platforms)

Lt. Col William Clay Moody, Ph.D.
(Software Development)

Sgt. Maj. Jeffrey Morris, Ph.D.
(Quantum Information/Talent Management)

Ms. Elizabeth Oren
(Cultural Studies)

Dr. David Raymond
(Network Security)

Dr. Paulo Shakarian
(Social Threat Intelligence/Cyber Modeling)

Dr. David Thomson
(Cryptographic Processes/Information Theory)

Dr. Robert Thomson
(Learning Algorithms/Computational Modeling)

Lt. Col. Natalie Vanatta, Ph.D.
(Threatcasting/Encryption)

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
NATO Cooperative Cyber Defence
Centre of Excellence

Dr. Michele L. Malvesti
Fletcher School of Law & Diplomacy, Tufts University

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

Shane Fonyi
Col. John Giordano

Lance Latimer
Eric Luke

Alfred Pacenza
Diane Peluso

Irina Garrido de Stanton
Col. J. Carlos Vega

CONTACT

Army Cyber Institute
Spellman Hall
2101 New South Post Road
West Point, New York 10996

SUBMISSIONS

The Cyber Defense Review
welcomes submissions at
CDR Manuscript Central

WEBSITE

cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published quarterly 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.

∞ Printed on Acid Free paper.

INTRODUCTION

COLONEL ANDREW O. HALL

09

Cyber Conflict in a Competitive World

SENIOR LEADER PERSPECTIVE

GENERAL JOSEPH L. VOTEL
MAJOR GENERAL DAVID J. JULAZADEH
MAJOR WEILUN LIN

15

Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR

ARISTEDES MAHAIRAS
MIKHAIL DVILYANSKI

21

Disinformation – Дезинформация (Dezinformatsiya)

PROFESSIONAL COMMENTARY

MATTHEW BEY

31

Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition

ANGELA MESSER
BRAD MEDAIRY

37

The Future of Cyber Defense... Going on the Offensive

RESEARCH ARTICLES

SUB-LIEUTENANT CHRISTOPHER ARGLES, ROYAL NAVY
EDITED BY PROFESSOR ED ZALUSKA

43

A Conceptual Review of Cyber-Operations for the Royal Navy

DR. ALEXANDER KOTT

57

Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks

DR. FERNANDO MAYMI
DR. SCOTT LATHROP

71

AI in Cyberspace: Beyond the Hype

RESEARCH ARTICLES

| | | |
|---|-----|---|
| ELIZABETH OREN | 83 | Culture in a Murky World: Hijab Trends in Jihadi Popular Culture |
| MAJOR ROCK STEVENS LIEUTENANT COLONEL JEFFREY BILLER | 93 | Offensive Digital Countermeasures: Exploring the Implications for Governments |
| COLONEL STONEY TRENT | 115 | Cultivating Technology Innovation for Cyberspace Operations |

RESEARCH NOTE

| | | |
|-------------------------|-----|---|
| DR. JAN KALLBERG | 137 | Supremacy by Accelerated Warfare through the Comprehension Barrier and Beyond: Reaching the Zero Domain and Cyberspace Singularity |
|-------------------------|-----|---|

BOOK REVIEW

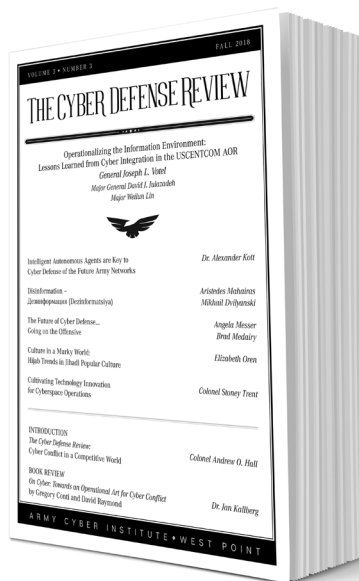
| | | |
|-------------------------|-----|--|
| DR. JAN KALLBERG | 145 | <i>On Cyber: Towards an Operational Art for Cyber Conflict</i> by Gregory Conti and David Raymond |
|-------------------------|-----|--|

THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

The Cyber Defense Review: Cyber Conflict in a Competitive World

Colonel Andrew O. Hall



INTRODUCTION

Welcome to, what we believe, is our most thought-provoking edition of *The Cyber Defense Review* (CDR). Before we begin this edition of the CDR, I would like to start off by extending my sincere thanks to those who put together the CyCon U.S. conference. This year's event at the Ronald Reagan Building in Washington, DC provided a dynamic environment to address relevant cyber issues confronting the global cyber community. Dr. Ed Sobieski and the CyCon U.S. conference committee continue to build a monumental event for cyber practitioners.

The CyCon U.S. conference also played host to the CDR's inaugural Editorial Board meeting. As Editorial Board Chair, I am humbled by the quality and expertise of our international board members of distinguished scholars and cyber leaders. The CDR Editorial Board give direction, discuss how to improve quality and reach, and serve as a channel for qualified input to increase CDR standing and ensure the overall success of the CDR in becoming the journal of choice for cyber practitioners. The Editorial Board examined our partnership with JSTOR, reviewed the new ScholarOne process, identified topics for themed and special issues, and provided influence, support, and input to the CDR team.

To continue our cyber conversation, I'm proud to announce the establishment of the CDR Press. This new project will allow those within the cyber community the opportunity to publish innovative and thought-provoking works. This endeavor is in keeping with the ACI and CDR's tradition of advancing the body of knowledge. Our inaugural CDR Press publication is entitled "Nonsimplicity, The Warrior's Way" by B. J. West and

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 53 person multi-disciplinary research institute and serves as the Chairman of the Editorial Board for *The Cyber Defense Review* 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.

D.C. Arney and will be part of a Security Studies Series. Our CDR Press will also publish important research studies, government reports, and conference proceedings for the cyber community.

Moving on to the CDR's Fall edition, I believe the contributors have ushered in a brilliant new standard of work for CDR readers. This issue features a leadership perspective from General Joseph Votel, Commander, U.S. Central Command, Maj Gen David Julazadeeh, and Maj Weilun Lin that address lessons learned from integrating cyber in the CENTCOM AOR, and offers compelling recommendations for operationalizing information across the joint community. Aristedes Mahairas and Mikhail Dvilyanski, of the FBI Cyber Branch in New York, lead us on a troubling exploration of Russia's disinformation campaign against our Nation.

We feature a professional commentary from Angela Messer and Brad Medairy, both senior cyber executives with Booz Allen Hamilton that provide a dramatic portrayal of 'Advanced Threat Hunting.' Matthew Bey, Senior Global Analyst at Stratfor, addresses superpower competition in the cyber domain.

We are proud of our six scholarly research articles. Dr. Alexander Kott, Chief Scientist at the Army Research Laboratory, presents a study on the value of intelligent autonomous agents for the cyber defense of Army networks; Dr. Fernando Maymi and Dr. Scott Lathrop take a critical look at artificial intelligence; CDR readers will enjoy Rock Stevens and Jeffrey Biller's research on offensive digital countermeasures and its implications for governments; COL Stoney Trent's article highlights the criticality of innovation to cyberspace operations; and readers can also look forward to a first-of-its-kind look into the Royal Navy's cyber operations with an article from Sub Lieutenant Christopher Argles RN. The research

commentaries are rounded out by a brilliant piece from Elizabeth Oren, Chief of Cyber Analytics at Jacobs' Mission Operations Group, which highlights the role of social media in Jihadi culture.

The CDR continues with our high-velocity research note section with an exciting work from Dr. Jan Kallberg and his examination of 'cyber supremacy.' If you are looking for another excellent read, Dr. Kallberg review of *On Cyber: Towards an Operational Art for Cyber Conflict* suggests why it should be on your reading list this fall. As always, we are excited to continue the cyber conversation together. ♥

THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆

Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR

General Joseph L. Votel

Major General David J. Julazadeh

Major Weilun Lin

INTRODUCTION

From Joint Publication (JP) 3-13, the Information Environment (IE) is defined as “an aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.” It is within this environment that our adversaries have engaged us persistently below a threshold that could trigger a kinetic response. Within the IE, the cyberspace domain provides our adversaries an asymmetric advantage where they can operate at the speed of war without bureaucratic obstacles or concern for collateral damage, and at relatively low cost. Rapid technological advancements and the lower barriers of entry open the cyber environment for both state and non-state actors to gain and exploit information. To respond to the unique challenge posed by the IE, we consolidated our lethal and non-lethal fires under one single portfolio in our Operations Directorate. This allowed us to maximize impact by synchronizing and integrating multi-domain operations during lethal and non-lethal planning and execution. With the full spectrum of lethal and non-lethal fires linked under one roof, we are better able to connect, integrate, and synch activities along with other Combatant Commands, the broader inter-agency, and the intelligence community. This integration makes us more lethal and disruptive at greater speeds and with greater reach resulting in hundreds of integrated Cyberspace Operations (CO) against our adversaries.

Contesting the information environment

Cyberspace as an operational domain is a relatively recent development in the evolution of US military warfare. Leveraging this new domain to enhance the effectiveness of military operations and contest the adversary requires an adjustment of

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



General Joseph L. Votel serves as the Commanding General of U.S. Central Command, MacDill Air Force Base, Florida, where he oversees an area of responsibility that stretches from north-east Africa, across the Middle East, to Central and South Asia.

The twenty countries within this vast region confront profound social, economic, and political upheaval while simultaneously facing grave security challenges in the form of widespread conflict, expansionist regional powers, violent extremist organizations and destabilizing behavior from outside actors.

GEN Votel is a graduate of the United States Military Academy, Infantry Officer Basic and Advanced Courses, United States Army Command and General Staff College, and the United States Army War College.

current cyber policy, the delegation of cyber operational authorities, expansion of cyberspace security cooperation, organizational doctrine, and interagency synchronization/coordination processes.

At USCENTCOM, we have discovered that Commanders must drive integration and synchronization of lethal and non-lethal capabilities across all domains – Land, Air, Sea, Space, and Cyberspace – in order to fully engage the adversary and create multi-domain dilemmas at the speed of war. In the past, our Information Related Capabilities (IRCs) were generally integrated as an afterthought into fully constructed operational and tactical plans. IRCs are “the tools, techniques, and/or activities employed within the IE that can be used to create effects” and include, for example, Cyberspace Operations (CO), Electronic Warfare (EW), Military Deception (MILDEC), Military Information Support Operations (MISO), Public Affairs (PA), and Civil Affairs (CA).

Over the last two years, we revised our approach and deliberately incorporated and integrated IRCs into our tactical to strategic level plans, developed a significant number of cyber and IO tools, and re-defined our Tactics, Techniques, and Procedures (TTPs) to fight our adversaries in this complex and volatile theater. As we continue to advance our abilities to engage in the IE and normalize how we operate within the Cyberspace domain, we need to proactively execute cyberspace and information operations early in “Phase 0 / steady state” of the planning process – well before operation execution. Only then can we shape the IE, hold our adversaries’ capabilities at risk, and execute at the speed of war.

Normalizing the cyber domain

My goal is to mature CO within our Command in a way that fully integrates cyber with the physical



Major General Dave Julazadeh is the Director of Plans, Policy, Strategy, and Capabilities, Headquarters United States European Command, Patch Barracks, Stuttgart, Germany. He is responsible to the USEUCOM Commander to formulate, provide staff direction and execute military/political strategy and policy, deliberate planning and security cooperation for command activities involving other U.S. Unified Commands, allied and partner military organizations and subordinate commands. He leads USEUCOM implementation of capability development, theater force posture, countering weapons of mass destruction and partnering programs within the command's area of responsibility.

He has served as an F-16 instructor pilot, functional check flight pilot and flight examiner logging over 2,500 flying hours and over 600 combat hours during Operations Provide Comfort, Deny Flight, Northern Watch, Allied Force, and Freedom's Sentinel.

domains and reduces “stove-piping” and “IRCs as an afterthought” common in the past. By doing so, we strengthen unity of effort in the USCENTCOM AOR and better posture cyberspace forces to support future campaigns, contingencies, and functions. We must not see Cyberspace as drastically different and separate from other domains that we create new processes to prepare, plan, and fight in this new domain. We continue to seek processes that smooth and simplify operations, reducing friendly friction and accelerating decision-making in order to meet the speed of the IE. We have achieved significant successes through better integration horizontally and vertically with stakeholders, which translates into non-kinetic impacts delivered more rapidly in support of the warfighter.

At the tactical level, we have integrated CO and fielded cyberspace capabilities to support Special Forces and, more recently, conventional ground forces. These tactical cyberspace and EW capabilities are synchronized with the ground scheme of maneuver providing an additional level of force protection to the warfighter by disrupting the adversaries' ability to command and control their forces in the battlespace. During our operations to defeat ISIS, our first success at true multi-domain operations through synchronized lethal and non-lethal effects was against ISIS's critical media operatives; we denied key infrastructure and degraded their ability to execute external operations through social media. These operations against ISIS have informed efforts across CENTCOM as well as other Combatant Commands.

Across the Central Command AOR, we are targeting Violent Extremist Organizations (VEO) propaganda distribution capability and command and control networks. On a daily basis, as our forces are operating in hot spots like Afghanistan, Iraq, and



Major Weilun Lin is Chief of the Central Asia and South Asia Cyberspace branch, Joint Cyberspace Center, Operations Directorate, United States Central Command, MacDill Air Force Base, Florida, where he plans and synchronizes cyberspace authorities, effects and capabilities for combat and contingency operations in the USCENTCOM area of responsibility.

Major Lin's notable staff tours include 17th Air Force (U.S. Air Forces Africa) as Chief, East and Central Africa Communications Engagement and at the 25th Air Force as the Chief, Air Force Intelligence

Community Security Coordination Center. Major Lin was commissioned through the Air Force Reserve Officer Training Corps at Texas A&M University, College Station, Texas.

Syria. Cyber Operators from CONUS Mission Centers, linked via chat, provide critical overwatch and are routinely demonstrating responsiveness at the tactical level. Further, cyberspace-enabled Military Information Support Operations (MISO) deliver content to discrete or broad target audiences giving us another venue to contest and compete in an environment. Combined, these efforts disrupt VEO C2, support and enable kinetic operations, and provide an opportunity to respond directly to high profile attacks, false claims of victory or simply to provide maneuver space (time) for US and Coalition forces to disseminate the facts.

Our intelligence community is a critical component of placement and access to physical and virtual infrastructures. Integrating the IRCs into the planning process early on is dependent upon accessing cyberspace-related intelligence which requires greater Cyberspace-ISR authorities throughout our AOR. Requesting and gaining those early authorities allow for the shaping of the cyberspace domain to occur in Phase 0 of operations to keep pace with the constant restructuring of this man-made domain. Within Phase 0, activities such as access, exploitation, deterrence activities, surveillance, and reconnaissance need to occur in order to support combat operations. These continuous discovery and analysis activities within the IE also support staff estimates and military decision-making, ultimately allowing the commander to selectively apply and maximize his combat power at the time and space of his or her choosing. Additionally, we've taken great care in refining our targeting processes to enable the execution of lethal and non-lethal fires from conceptualization of the plan to execution. Normalizing CO requires us to treat cyberspace-related intelligence and target development the same as other warfighting domains.

Lessons learned

Modern conflict requires streamlined processes, rapid deployment of technology, complementary partnerships, and flexible authorities to fully leverage cyberspace as an operational domain. CO uniquely requires those authorities, capabilities, and permissions early in Phase 0 to gather intelligence and operationally prepare the information environment. Improvements in the targeting process and synchronizing the IRCs provide the Command with processes that are robust enough to react to adversary actions but nimble enough to seize upon emerging opportunities. Just as on the kinetic battlefield, our enemy is highly adaptive in their cyber TTPs. While our cyber operations have been technically successful, authorities, capabilities, and permissions currently inhibit us from significantly increasing the overall effects in the information environment.

We must leverage the incredible knowledge and strengths of interagency, industry, and academic partners to create better cyber capabilities that better enable our IRCs. We must prioritize to get properly resourced so that we can rapidly procure, develop, test, train, and field them to our forces. Our warfighters need tomorrow's technology today. We've made significant progress, especially over the last eighteen months, in gaining these authorities for the Combatant Commander. We have taken the lessons learned from our operations against ISIS and our successes in Afghanistan and applied them to subsequent operations to enable our warfighters to combat our adversaries. We have also shared these lessons and plans with other Combatant Commands such as U.S. Africa Command (USAFRICOM) in support of their operations against ISIS in the Sahel and other ISIS affiliates.

CONCLUSION

The continued advancements in technology have changed the employment and conduct of warfare; however, the fundamental nature of war remains the same. We are contested across all dimensions of power and must integrate the IRCs into how we fight. It is essential for Commanders in all domains to understand and incorporate the cyberspace domain across the other warfighting domains in order to disrupt the adversary's capabilities and will to wage war. Normalizing the cyberspace domain means broader authorities that are more responsive than current bureaucratic processes. It also means we need simple and streamlined organizations and processes to increase lethality and enhance performance. We need technology and capabilities to keep pace with the operational environment and continue to build the partnerships to do so. This also requires shaping the IE early and continuously so we hold our adversaries' capabilities at risk.

Today's commanders must drive integration of lethal and non-lethal effects across Land, Air, Sea, Space, and Cyberspace in order to create unity of action while maintaining our competitive military advantage on the battlefield. Our failure to operationalize and normalize the cyberspace domain effectively cedes it to our adversaries, gives them a competitive advantage, and ultimately, creates an increased attack vector against our objectives. 🛡️

Disinformation – Дезинформация (Dezinformatsiya)

Aristedes Mahairas
Mikhail Dvilyanski

Disinformation is defined by Merriam-Webster as “false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth.”^[1] The word disinformation did not appear in English dictionaries until the 1980s. Its origins, however, can be traced back as early as the 1920s when Russia began using the word in connection with a special disinformation office whose purpose was to disseminate “false information with the intention to deceive public opinion.”^[2] Russia considered disinformation as a strategic weapon to be used in its overall Active Measures strategy. Active Measures, активные мероприятия, is a Soviet term for active intelligence operations for the purpose of influencing world events to achieve its geopolitical goals.^[3] Major General Oleg Kalugin, retired KGB, considered disinformation as a critical component of the Active Measures strategy. Major General Kalugin described this as “the heart and soul of Soviet intelligence. Not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.”^[4] To achieve these ends, many different methods were employed; such as, the creation of front organizations, the establishment of opposition parties, the support of criminal and terrorist organizations, and even the spread of disinformation through official and unofficial channels designed specifically to sow discord among the targeted audience.

1960S: OPERATION NEPTUNE

Operation Neptune was one such example. In this 1964 disinformation operation, the Czechoslovak secret service, working with the KGB, participated in the sinking and

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



Special Agent in Charge Aristedes Mahairas heads the New York (NY) Special Operations/Cyber Division. He previously served as Legal Attaché, Athens; Joint Terrorism Task Force Supervisor; Section Chief, Strategic Operations Section-Counterterrorism Division; Chief of Staff to the Executive Assistant Director, National Security Branch. Prior to entry with the FBI, he served as a Police Officer in NY City and received a Bachelor of Arts degree in Political Science, Baruch College, and a Juris Doctor, NY Law School.

staged discovery of four chests of Nazi intelligence documents which had been forged and made to appear as if they had been under water since World War II. These documents were designed to discredit Western politicians by revealing names of former Nazi informants who were still being used as spies in Eastern Europe. Ladislav Bittman, the Czechoslovak agent who defected to the West in 1968, originally placed the documents in Cerne Jezero, the Black Lake, and later led the divers, who were part of a documentary team, to make the discovery. Bittman, who ran the operation stated, “It was the Cold War and the goal was to re-awaken interest and discredit West German politicians. Another goal was to have the statute of limitations for war criminals, which would have expired in 1965, extended. Following the extensive media coverage, the countries that suffered during WWII demanded that the statute be prolonged. Germany eventually extended it and then agreed that there be no limited time in which their war criminals could be tried.”^[5]

1970s: U.S.-EGYPTIAN RELATIONS

Another example of KGB active measures is the robust Soviet disinformation campaign against the U.S.–Egyptian relationship and the Camp David peace process in the late 1970’s. The campaign focused on derailing the Middle East peace process and exacerbating tensions, attempting to undermine U.S. standing and influence in the region. The KGB demonstrated aggressive use of forgeries during the campaign, including a forged document purportedly from the office of the U.S. Secretary of State for the U.S. President, using language offensive to Egyptian President Anwar Sadat and other Arab leaders. This forgery was anonymously delivered to the Egyptian Embassy in Rome in 1977. Also in 1977, a series of forged letters purporting to be official U.S. Government documents were delivered



Mike Dvilyanski served in the FBI from 2005 until 2018, most recently as Supervisory Special Agent at the Cyber Branch at the FBI's New York office. In this role, Mike led an investigative team focused on state-sponsored computer intrusions against U.S. interests and was responsible for the development and implementation of a cyber incident response framework for the FBI's New York office. Previously, Mike served as Supervisory Special Agent in the Cyber Division at FBI Headquarters in Washington, D.C., where he oversaw investigations of state-sponsored cyber threats. In 2017, Mike returned to FBI Headquarters to help lead the FBI's efforts to combat election interference and foreign influence operations. Mike graduated from the FBI Academy in 2005 and was assigned to the New York Field Office of the FBI, where he investigated Counterintelligence and Cyber matters.

to numerous locations. The letters advocated a “change of government” in Egypt and criticized President Sadat’s leadership. Finally, in 1979, a forged letter from the U.S. Ambassador to Egypt was published in a Syrian newspaper. The letter was critical of President Sadat and expressed the U.S. position of wanting to “get rid of him without hesitation.” The breadth and duration of this active measures campaign clearly illustrates the importance Soviet leadership placed on undermining US credibility and influence in the region as a key sponsor of the Camp David peace process.^[6]

RECENT EVENTS

Nearly 100 years after Russia established its special disinformation office, an analysis of recent events shows that such disinformation campaigns no longer require the sole services of intelligence operatives of old. In fact, with the leveraging of technology and the use of both overt and covert methods, such disinformation campaigns can have an even greater impact to a wider audience in a rather short period of time. It should be noted however that the purpose of such campaigns remains the same. The goal is to create discord and confusion, and amplify existing divisive issues in order to further expand the space separating the targeted audience; thereby, making reconciliation between any two sides of a divisive issue even more difficult to achieve.

2016: LISA CASE

One clear example of this activity, utilizing both overt and covert channels to propel a disinformation campaign, is evidenced in the Lisa case which takes place in Germany. For two weeks in January 2016, the media focused on Lisa, a 13-year old Russian/German girl, who had gone missing for 30 hours and was reported to have been raped by Arab migrants.^[7] The German police, as with any allegation

of a serious crime, quickly investigated this matter, and in very short order, determined the story to be false. In fact, Lisa herself admitted to having been with friends during the time in question.^[8] Despite the speed in which the German authorities were able to reach a logical conclusion, the story had taken on a life of its own.

SUCCESSFUL ALIGNMENT WITH SOCIAL MEDIA TO ACHIEVE DISINFORMATION

The Lisa saga began taking shape with Russia's state-sponsored Channel One which broadcasts into Germany in Russian. The story was then picked up by Russia Today (RT); RT Deutsch, and Sputnik. All three are well-known – overt – Russian government controlled media outlets. In fact, in 2017, RT and Sputnik registered with the U.S. Department of Justice under the Foreign Agents Registration Act (FARA) declaring their respective organizations as agents of a foreign power, to wit, Russia. This overt media activity was coupled with the covert actions of a Facebook group and anti-refugee website called Ayslterror, which was later determined to have links to Russia.^[9] The actions of this group spurred various social media and rightwing groups to widely distribute the information on the internet, to include demonstrations which were organized via Facebook involving representatives of the German-Russian minority (Deutschlandrussen) as well as neo-Nazi groups.^[10] This disinformation campaign focused on exploiting the existing divide among Germans as it related to the Arab-migrant issues and some speculate it was orchestrated and directed in response to Germany's leading role in the Ukraine crisis and Chancellor Merkel's subsequent stance on sanctions against Russia.

Whether it is the use of intelligence operatives in the field or intelligence operatives behind the keyboard, Russia has fully embraced a strategy of information warfare, one designed to achieve long-standing intelligence objectives in support of their overall geopolitical agenda. The Lisa case is one of a handful of cases that can be viewed as evidence that the Kremlin is engaged in a structured approach to leverage new age technologies.^[11]^[12]^[13] A thoughtful analysis of the methodologies employed reveals an organized model that serves as a framework for conducting foreign influence operations in the Information Age, and incorporates several logical steps to ensure maximum impact.

The influence campaign begins by identifying existing socially and politically divisive issues followed by the development of messaging themes to amplify these divisions along existing fault lines. The adversary then begins to establish the technical infrastructure and networks of influence, which will ultimately be used to publish and perpetuate the campaign. Simultaneously, affirmative efforts are undertaken to obtain and produce material that will yield the desired objective. Once the sought after information is obtained, through hacking, forgery, or “creative” content such as articles, blogs, or specifically designed news stories presenting false information, it is then published to the targeted audiences for public consumption.

At this stage of the campaign, the objective is to create confusion surrounding the true motivation behind the content and hide the origins and sponsorship by the foreign government. Subsequent to publication and consumption, the adversary will engage in a concerted effort to amplify the messaging. This intensification is powered by the modern information landscape and social media. Here, the adversary begins to achieve scale in order to sow discord, confusion, and doubt by saturating the information space and amplifying divisive issues that appeal to existing biases of the target audience.

The principle objective of this activity is to get unwitting audiences to engage with the influence content and disseminate it further within their own social networks, thus extending its reach. The effect of this total effort is ultimately analyzed by reviewing the impact on and engagement by the audience to assess the effectiveness of the influence campaign; this may undergo a period of fine-tuning to maximize its impact. The entire process and its ultimate success relies on the coordinated efforts of the numerous overt and covert actors who take part in the manufacture of stories and information designed to manipulate the masses.

Russia's 2016 US Presidential election influence effort highlights just how this methodical approach is precisely implemented. Bill Priestap, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation stated, "Russia's 2016 presidential election influence effort was its boldest to date in the United States. Moscow employed a multifaceted approach intended to undermine confidence in our democratic process ... which included the weaponization of stolen cyber information, the use of Russia's English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging."^[14] This statement clearly highlights the use of overt and covert means to create multiple false narratives designed to work together to shape the perception of the target audience.

A key objective of modern influence operations is to make true facts harder to find and garner consensus. The goal is to not just to present an alternate version of reality, but rather to contaminate the information space with many such versions, some of them conflicting, to confuse the audience and erode its ability to think critically. It is about creating a sentiment that no news source or narrative can be trusted and providing fodder to the audience to connect with whichever storyline most appeals to its pre-existing biases. It is about diminishing our collective ability to find the truth and agree on it. The modern information landscape allows for this to be achieved rapidly and at scale, by delivering false narratives directly to the audience much more quickly and broadly than was ever possible before. Achieving this objective is made easier when nearly two-thirds of American adults are getting at least some of their news on social media and where the act of sharing a piece of content (such as a post, a news story, or a meme) within one's own social network can often be more important than its veracity.^[15]

If we are to avoid the toxic consequences of disinformation, we need to sharpen our sense of skepticism and ask pertinent questions about the veracity and motivation of what we view and share. We need to engage in transparency and expose this behavior, shining a spotlight on it whenever we can. Education of the threat and providing context to enable critical judgment will help mitigate this vulnerability. Otherwise, if we do not challenge the dissemination of falsehoods, we not only allow, but also invite ill-intentioned forces to continuously negatively influence us all. 🛡️

NOTES

1. “Disinformation” Merriam-Webster.com, Merriam-Webster, n.d. Web, June 3, 2018.
2. Ladislav Bittman, “The KGB and Soviet Disinformation: An Insider’s View,” Pergamon-Brassey’s, 1985.
3. Christopher Andrew and Vasili Mitrokhin, “The Mitrokhin Archive: The KGB in Europe and the West,” Gardens Books, 2000.
4. Oleg Kalugin, CNN Interview, Archived at the Wayback Machine, 2007.
5. Ladislav Bittman, “The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare,” Syracuse University Research Corporation, 1972.
6. United States Department of State, Special Report No. 88, “Soviet Active Measures: Forgery, Disinformation, Political Operations”, 1981.
7. Stefan Meister, “The ‘Lisa Case’: Germany as a target of Russian disinformation,” NATO Review, <https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm>.
8. Ibid.
9. Alina Polyakova and Spencer P. Boyer, “The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition,” Foreign Policy at Brookings, 2018.
10. Stefan Meister, “The ‘Lisa Case’: Germany as a target of Russian disinformation,” NATO Review, <https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm>.
11. Neil MacFarquhar, “A powerful Russian weapon: The spread of false stories,” The New York Time, August 28, 2016, <https://www.nytimes.com/2016/08/29/world/wurope/russia-sweedden-disinformation.html>.
12. United States of America v. Internet Research Agency LLC et al., <https://www.justice.gov/file/1035477/download>.
13. Joseph Menn, “Exclusive: Russia used Facebook to try to spy on Macron campaign – sources,” Reuters, July 27, 2017, <https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBNIACOEL>.
14. Bill Priestap, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Statement Before the Senate Select Committee on Intelligence, Washington, D.C., June 21, 2017, <https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections>.
15. <http://www.pewresearch.org/fact-tank/2017/10/04/key-trends-in-social-and-digital-news-media/>.

THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆

Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition

Matthew Bey

Earlier this year the Pentagon released its first National Defense Strategy in a decade. The document put the long-term great power competition between the United States and what it calls two revisionist powers, China and Russia, at the forefront. Russia's global influence on the global stage has been steadily resurging over the past ten years, culminating with its intervention in Ukraine in 2014, and China, likewise, has regained its historical status as a global power after its so-called century of humiliation. Though the United States' attention has been elsewhere – namely on the Middle East and the Global War on Terrorism – for much of this time, it is now renewing its focus on its near peers in a return to the status quo.

Cyberspace will be a critical battleground for the United States, China, and Russia as they jockey for global influence. The domain is, of course, a relatively new environment where the governing norms and treaties are still only in their infancy and not universally accepted. And because the United States, China, and Russia are by far the three greatest cyber powers worldwide, the rivalry between them will define the treaties and norms that develop. The process will take time, and it could get messy.

The three parties involved diverge significantly in their views of issues such as how to apply international law to cyberspace, the extent of national sovereignty over cyberspace, and the nature of human rights within it. As the global competition increases, we can expect these topics to become only more polarizing. The U.N. Group of Governmental Experts failed miserably last year in trying to gain consensus on these points of contention. After all, the difference in US, Russian and Chinese viewpoints on cyberspace are rooted in the three countries' very different geopolitical imperatives and constraints.



Matthew Bey is a senior global analyst at Stratfor, an Austin, Texas-based geopolitical intelligence firm, where he leads the company's analysis on international trade, economics, energy, emerging technologies, and related trends with an emphasis on China, the Middle East and Africa. Mr. Bey holds a master's degree in mathematics from The University of Texas at Austin and a bachelor's degree from Texas Lutheran University.

CHINA'S MULTIFACETED STRATEGY

China's overall strategy toward cyberspace consists of several layers. First, the country's view of the global system and its relationship to the great power competition shapes how aggressive Beijing will be in promoting its viewpoint. China today is seeking to revise the US-led international system to have greater prominence, having spent much of the twentieth century in the periphery and largely excluded from developing global norms. Much as Beijing views the dollar-backed international financial system as evidence of the United States' entrenched power, it considers the application of US law to other countries and the Western interpretation of international law on Internet freedom as a way for Washington and its allies in the West to assert their influence worldwide. The size of its market gives China the power to dictate the terms of doing business there, making the discussion over cyberspace standards one of the first where Beijing has a seat at the table to legitimately argue that it is a peer competitor of the US and, as such, an important voice in the debate.

That does not mean, however, that China wants to break the current system. Quite the contrary. The country's economic and social stability depends on the continuation of the status quo. Global trade flow, information flow, and interconnectivity underpin China's economy as much as they do the US economy. For that reason, China views the ad hoc bilateral deals it has struck over its cyber policies – such as the 2015 agreement with the United States to halt cyberattacks used for industrial espionage – as necessary to defuse tensions with other countries while avoiding disruptions. These types of agreements will also become increasingly important to China as it develops technology that it seeks to protect from industrial espionage, regardless of whether it abides

by these deals. China's priority is to ensure that international cyber norms don't evolve in such a way that its domestic policies become a liability.

Second, China's strategy over cyberspace is closely tied to its national security. It's no secret that the Chinese government has tried to control the flow of information for decades to maintain rigid governance of its expansive territory and large population. To update that campaign for the twenty-first century, Beijing has developed a sophisticated cyber strategy. External threats – whether from an outside power such as the US or a domestic opposition group – have long been a catalyst for unrest (consider the 1989 Tiananmen Square uprising, for example, or the more recent protests in Ukraine, Central Asia, and the Arab world.) In the information age, China worries that hostile forces could use the internet to undermine the Communist Party's authority and destabilize the country with a cyberattack or merely the dissemination of information. President Xi Jinping's administration has taken steps to mitigate that risk, tightening censorship to enhance ideological conformity and to suppress political dissidents during the difficult socio-economic transition underway in his country.

As China gears its strategic environment toward the growing competition with the United States, Beijing will further strengthen its grasp on domestic cyberspace through measures such as data localization laws. At the same time, Beijing will likely intensify its online intelligence gathering. Its intrusions this year into US maritime companies' data and various political groups in the run-up to Cambodia's elections have showcased its expanded collection efforts.

Third, China's cyber strategy corresponds to its industrial policy. Though China's capabilities in cyber operations and emerging technologies such as artificial intelligence are becoming more sophisticated, the country still depends largely on Western technology. Beijing is hoping to break that dependency through the Made in China 2025 plan. Just as the United States worries that products from Chinese tech companies Huawei and ZTE may include backdoors that Beijing can exploit, China has reason to believe that Western technologies will give foreign intelligence agencies a way into the country. The US, in response, is working to pressure Beijing into abandoning its techno-nationalist ambitions; a recent example is its proposal to expand the jurisdiction of the Committee on Foreign Investment in the United States to include export controls on industrially significant emerging technologies.

These attempts, however, will only push the Chinese government to redouble its efforts to develop its own tech giants, including conducting industrial espionage as needed, despite the 2015 deal with Washington. Given the increasing convergence between the tech and defense sectors, the Chinese military will take on a larger role in supporting China's tech pursuits. Its involvement will give China a competitive advantage over the US, where a gulf remains between the military and Silicon Valley.

RUSSIA: THE NOT-SO-NEAR PEER

Like China, Russia bases its cyber strategy in large part on its need to resist external influence. Both countries encompass large territories and disparate populations that over time have defied centralized government. To manage that challenge, Moscow, like Beijing, has historically restricted the flow of information to its public as a means of controlling the population; it is similarly concerned about rivals using information against it, even more so since the color revolutions across the former Soviet Union during the previous decade. Russia, therefore, shares China's belief in national sovereignty over cyberspace, though it is perhaps more focused on information warfare than the threat of tactical attacks and physical disruptions.

In other respects, Russia's cyber strategy differs from that of China. For one thing, it is an interventionist strategy, in line with Russia's interventionist foreign policy. Russia and China alike use cyber operations for general intelligence gathering, but Moscow has also used them to conduct large-scale disinformation campaigns overseas, most notably ahead of elections in countries such as the US and France. For another, Russia is not the near-peer economic competitor to the US like China. A growing number of obstacles stand in the way of its achieving that status. Along with the economic stagnation caused by the 2014 crash in oil prices, the country is in the throes of a demographic crisis that will reduce its population by 2.4 percent by 2030.

Russia is a leader in certain cyber capabilities, and it does have a few well-established technology companies on the software side of things. Nonetheless, it simply does not have the commercial industry that China and the US have to support tech development. The Russian Google or Huawei does not exist, and it probably never will. Consequently, the Kremlin will have to rely on the levers it already has at its disposal to achieve its goals regarding China and the US, namely cyberattacks and disinformation campaigns. These relatively low-cost tactics will remain a key feature of Russia's cyberspace policy going forward, even though the West will continue to develop more sophisticated response mechanisms to counteract them.

THE DEBATES TO COME

The return of near-peer competition will not result in the bipolar international system of the Cold War; the economies of China, Russia, and the US are too deeply intertwined to enable that outcome. Although the intensifying rivalry among the US, China, and Russia stymied the U.N. Group of Governmental Experts, it does not necessarily preclude the establishment of international norms on cyberspace. Instead, it will merely limit their scope.

Despite international concerns over state-sponsored cyberattacks, the use of intrusive tactics such as hacking, for political or military gain, has become more or less an accepted fact of life in the internet age. Industrial espionage, likewise, is emerging as a red line

in the cyberspace discussion because of China's pragmatic stance on the issue. Norms around operations that either physically disrupt business operations or cause physical damage will be hard to hammer out. The US, China, and Russia have all been deliberately vague about where they would draw the line on unacceptable practices, an approach that is not exactly conducive to establishing clear global standards. Nevertheless, norms will eventually materialize, even if they are hazy and largely implied since few treaties or enforceable agreements are likely to come about to implement them. The West's push for a rules-based system or a central body, like the World Trade Organization, to govern cyberspace and adjudicate on complaints will probably be a non-starter for China. Furthermore, Beijing and Moscow would have more to lose than to gain from joining such an institution and relinquishing control over their domestic cyberspace.

In short, the rules of cyberspace probably will remain ad hoc and muddled as the geopolitical competition heats up. It is unlikely that China would support the creation of well-defined cyber norms in the context of the Western-led international system. Both China and Russia, meanwhile, will continue to try to exploit the gaps in cyberspace governance to further their objectives. These countries will, for example, keep using mercenaries and cyber proxies to carry out cyber operations on their behalf so they can circumvent existing norms in cyberspace while maintaining plausible deniability.

Under these uncertain conditions, the Balkanization of cyberspace and of the technology sector, which have manifested so far in the push for data localization, will likely continue. The absence of a global rules-based system governing cyberspace means that the differences in laws, regulations, and litigation practices from state to state will only grow as countries try to exert greater control over the internet.

The escalating great power competition between Russia, China, and the US will shape the evolution of cyberspace and of the conventions surrounding it. Though Moscow will have its role to play in the process, Beijing and Washington will largely determine its outcome as they embark on what is likely to be a lengthy period of economic, military, technological and political rivalry without precedent since the Cold War. 🇺🇸

The Future of Cyber Defense... Going on the Offensive

Angela Messer
Brad Medairy

ABSTRACT

Today, organizations are faced with the overwhelming challenge of protecting their enterprise against threat actors that are well resourced and constantly evolving. While most clients have a traditional Security Operations Center (SOC) to identify vulnerabilities and catch harmful activity on their networks, historical evidence proves that perimeter defense alone is not enough. To combat these evolving threats, traditional approaches to Cyber defense must evolve, and enterprises must go on the offensive. One emerging approach is Advanced Threat Hunting. An approach that pairs best-in-class Cyber Defense tools with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Advanced Threat Hunting, in conjunction with the client's current security posture, offers a proactive, defense in-depth solution focused on finding malicious actors.

TODAY'S CYBER SECURITY LANDSCAPE

Does it help you sleep thinking that your cyber team has a plan to respond after you've been hacked? It shouldn't. Your organization may have used a "react-and-defend" approach to cybersecurity for years. However, if you think this strategy is enough to protect your organization from a breach, you're wrong.

Too many organizations wait to be notified that they've been breached. Yet with the increasing number and scale of cyberattacks—and the sophisticated techniques threat actors are using to mask their activities—the traditional approach of "building bigger fences" will no longer suffice.

The hack of Equifax in 2017 posed one of the most significant risks to personally sensitive information in years, potentially exposing data for as many as 143 million



Angela Messer is an Executive Vice President and Chief Transformation Officer (CTO) for Booz Allen Hamilton. Before being named CTO in April 2018, she led the company's Cyber capability, guiding teams of cyber forensics engineers, data scientists, and threat intelligence experts who focus on cyber malware, cyber next gen operations, and incident response. Angela also led the Firm's Army business, which is a global, multi-functional business in the defense and intelligence sector. Prior to joining the company, she was a U.S. Army officer, managed two major commercial businesses and launched a startup software development company. She earned a B.S. in engineering management from West Point Military Academy and an M.S. in management from the Florida Institute of Technology.

Americans, according to the New York Times.^[1] High profile, large-scale breaches like the one at Equifax serve as reminders that a defensive cyber approach is no longer sufficient.

Today's Advanced Persistent Threat (APT) actors commonly engage in long-term campaigns to compromise target networks, seeking first to gain, then maintain, a hidden presence. APT actors are skilled at defeating reactive, rule-based cybersecurity defenses by continually evolving their malicious tools, techniques, and procedures (TTPs). Modern polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and operating system hijacking techniques all evade traditional defenses.

COMMON CHALLENGES WITH EXISTING CYBER DEFENSE APPROACHES

While a tremendous amount of dollars and resources have been invested to secure the enterprise, Cyber defenders struggle to keep pace with sophisticated adversaries that are continually evolving their tactics at little cost. Enterprises are continually looking to the vendor community to provide the "silver bullet" in the form of a security product that will make this problem disappear. Unfortunately, this has further amplified the problem. Security teams are stretched thin monitoring the numerous products necessary to provide traditional perimeter defense. As no single device or platform provides the complete solution, they are stuck with an "eyes on glass" approach.

Most enterprises today have turned to Security Information and Event Management (SIEM) platforms to help analysts better triage and identify high priority events; however, this too is failing. Analysts are either flooded with false positive alerts, known as alert fatigue, or the platform is over tuned and missing true positive alerts. In both scenarios,



Brad Medairy is a McLean, VA-based Senior Vice President and leader in Booz Allen's Strategic Innovation Group (SIG) focused on the delivery of Cyber solutions across Federal and Commercial clients. In this role, Mr. Medairy is responsible for the development and delivery of next generation service offerings that integrate Booz Allen's leading Cyber (e.g., Malware Analysis, APT Hunting, Incident Response, Security Operations Center design & support), Engineering, Systems Development (e.g., Reverse Engineering), and Data Science capabilities. Mr. Medairy engages with clients across the Defense and Intelligence Community, Federal Agencies (e.g., Department of Homeland Security), and commercial market (retail, financial services, automotive, energy/utilities, and pharmaceutical) to understand their current environment, assess the threat landscape, determine their risk posture, and deliver tailored solutions that address their business/mission requirements

critical events are likely to be missed. Most enterprises do not truly know if they are compromised and are unaware if cyber threats are "living off the land." It's often difficult to assess how far a threat actor has crawled across an enterprise. For all they know, advanced actors lay dormant, quietly moving laterally, conducting reconnaissance, and ex-filtrating sensitive data undetected.

GOING ON THE OFFENSIVE

In today's unpredictable environment, filled with rapidly evolving threat actors and emerging technologies, the only way organizations can protect themselves is by unleashing offensive cyber techniques to uncover advanced adversaries on their networks. The most effective approach—**advanced threat hunting**—is essential to any organization that wants to stop and prevent attacks in its networks.

Advanced adversaries live in the noise of networks and defeat reactive, rule-based cybersecurity defenses by constantly developing malicious tactics, techniques, and procedures (TTPs). These developments—such as polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and hijacking legitimate operating system functions—all evade traditional defenses.

In working with clients on hunt engagements, we have found an average dwell time—that is, the time an advanced adversary lies undetected in a victim's network—of 200-250 days before discovery. Advanced threat hunting involves actively searching for compromises before alarm bells go off by carefully combing through networks and datasets to discover hidden threats. By regularly evaluating their networks for threat activity, organizations can catch attacks in progress—before it's too late. Advanced threat hunting is a proactive approach that relies on sophisticated tools and tradecraft,

such as automation, threat intelligence, threat analytics, and machine intelligence, to gather and analyze vast reams of data. Advanced threat hunting uncovers threats that are generally invisible to the traditional network security, endpoint security, and perimeter defenses at the core of anomaly detection. The focus of threat hunting is to reduce the dwell time (the length of time between initial breach and expulsion of the threat from the network) of APTs that are missed by the client's SIEM, intrusion detection system, and/or Anti-Virus solutions. While threat hunting leverages the client's SIEM, it's important that the data not be filtered so that the high false positive data, where indicators of a skilled APT will exist, can be revealed. Potentially malicious events are identified through Indicators of Compromise (IOCs), hypothesis-based rules that allude to a persistent threat's TTPs, and anomaly detection analytics supported by machine intelligence. Threat hunting is most effective when employed in real-time, but it can be used like a Compromise Assessment to analyze historical data for signs of a breach. These tools can identify and mitigate threats at machine speed using customized delivery models.

It is important to note that not all threats can be detected with automated tools alone. These tools must be paired with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Threat analysts can make sense of complex data, develop hunting hypotheses, and test these hypotheses to better identify hidden threats.

Even with trained analysts using the right tools, ad-hoc hunting isn't enough—it must be standardized and measured. Advanced threat hunting requires implementing a repeatable process that's part and parcel of an organization's overarching security strategy. Fusing Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools intelligently can help to streamline this process.

CONCLUSION

At Booz Allen, we have spent the last decade assembling teams of analysts who can think like the enemy and know how to identify warning signs. Our analysts specialize in global malware hunt operations, anti-malware research, and development of APT countermeasures, and use measurable processes to strengthen network defenses and identify adversary activity.

Incidents like the Equifax hack don't have to be inevitable. Organizations need to take steps now to improve their security posture before the next attack hits. Three elements—analytical tools, talented threat analysts, and a standardized hunt process embedded in a broader security strategy—can be the key to knowing your organization is protected. With advanced threat hunting, you can sleep well at night—or at least a little better. 🛡️

¹<https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>

THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆

A Conceptual Review of Cyber-Operations for the Royal Navy

Sub Lieutenant Christopher Argles RN
Edited by Ed Zaluska

ABSTRACT

Cyberspace is a malleable and seemingly ubiquitous environment through which information flows. Armed forces use this information to make decisions and take action. The fundamental importance of cyberspace to modern military operations leads threat actors to desire access to and control over its components. In response, organizations like the Royal Navy conduct defensive Cyber-Operations (CO) to protect their information networks and platforms. At the same time, offensive CO allow armed forces to take advantage of the reach of cyberspace to weaken the position of their adversaries. This paper discusses the nature of the threats faced by national-security institutions, and the doctrinal factors that policy-makers must consider. The paper reviews the approach to CO of several countries and evaluates the work done by the Royal Navy in developing cyber capabilities.

I. INTRODUCTION ABSTRACT

1.1 Problem statement

Little information exists in the public domain about any of the Cyber-Operations (CO) conducted by the British Armed Forces. The sensitive nature of the deployment of cyber capabilities for military purposes requires that access to these details remains under tight restrictions. Nevertheless, a few publications by the Ministry of Defence (MOD) provide an insight into the approach to CO adopted by the Armed Forces. This material discloses some of the high-level concepts about training, organizational structures, and policy.



Sub Lieutenant Christopher Argles serves as a Junior Officer in the Weapons Engineering branch of the Royal Navy. Sub Lieutenant Argles joined the Royal Navy as a Midshipman under the Defence Technical Undergraduate Scheme in 2013. In 2016 he spent a period attached to the Information Directorate of the United States Air Force Research Laboratory to research information assurance and deception in contested cyber environments. He graduated from the University of Southampton with a Master's Degree in Computer Science with Cyber Security. Upon receipt of his commission from Britannia Royal Naval College, he was selected to join the Submarine Service and undertook the Weapon System Engineering and Management Course at HMS COLLINGWOOD. In his current role, Sub Lieutenant Argles supports maritime C4ISR operations.

A discussion of the ideas presented by the MOD, and a comparison of the UK approach with that of other countries, provides an insight into the evolution of current doctrine. However, there appears to be very little evidence of this in the open literature.

This paper draws upon several cyber reports, policy documents, and academic papers to highlight some of the key factors that affect CO and to set out recommendations for policy-makers to consider. The Royal Navy is selected as the focus of this paper because of the challenges associated with the conduct of maritime CO, in addition to the author's background as a Naval Officer. Interviews with members of the Royal Navy's new Cyber Defence Operations Centre (CDOC) and attendance at INFORMATION WARRIOR 17 (IW 17) enable this paper to provide a privileged evaluation of the work undertaken by the Royal Navy in implementing the tactics, techniques, and procedures required to deliver an operational cyber capability.

1.1 Contributions

Section 2 presents a background to current threats and threat actors in cyberspace and discusses how they affect national security. This section also highlights the need for policy-makers to understand the type of randomness that applies to CO. Section 3 summarizes the approach to CO adopted by the United States Department of Defense (DoD), China, and Russia. The report then provides an overview of the work done by the United Kingdom and the Royal Navy in the development of CO doctrine and capability. Section 4 looks at how the Royal Navy recruits and trains the individuals who serve in cyber roles. Moreover, the section details the potential contribution that "Capture the Flag" (CTF) competitions might make towards improving the preparedness of cyber personnel. From the evaluations in Section 3 and 4, the report sets out several recommendations to inform future discussions on Royal Navy CO doctrine.



Ed Zaluska is an Associate Professor in Electronics and Computer Science at the University of Southampton (UK) and a Life Senior Member of the IEEE. His current research interests embrace cybersecurity and all security aspects associated with distributed systems.

1.3 Limitations

This paper provides an open review in the unclassified domain of the CO doctrine of several major powers, intended for cyber policymakers and CO researchers. Specific details about technical capabilities and associated deployments remain outside the scope of this evaluation. Because of this, some of the conclusions and recommendations presented in this report might not apply in full to the Royal Navy but should be interpreted as proposed guidelines and principles for future consideration.

2. BACKGROUND

2.1 Definitions

While many definitions of cyberspace exist, this report (unless specified in the context of national doctrine) uses the definition provided by Ormrod and Turnbull:

“an evolving loosely bounded and interconnected information environment that utilizes technologically mediated software-enabled methods of communication” ^[1]. As defined in the MOD Cyber Primer, CO refers to “activities that project power to achieve military objectives in, or through, cyberspace” ^[2].

2.2 Current threats

Alongside terrorism, and interstate conflict, the 2015 Strategic Defence and Security Review listed cyber threats to the United Kingdom and her interests as a ‘Tier One’ (highest priority) risk to national security ^[3]. As computer technologies and information networks continue to increase across naval platforms (ships, submarines, etc.) and supportive infrastructure (information services, logistics, education, etc.), the Royal Navy becomes ever more dependent on the assured functionality of these systems ^[4].

Muti and Tajer provide some real-world and hypothetical scenarios to illustrate the types of CO which threaten national security institutions like the Royal Navy ^[5]. Their report cites a consensus among scholars that the impact of CO on national security is often exaggerated ^[6]. We wish to highlight those CO that pose a genuine threat.

The most serious concern is the discovery of vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) technology used in Critical National Infrastructure (CNI) and in military platforms that provide an interface between a user and machinery. The report describes how these vulnerabilities facilitate the use of sabotage CO by state-supported threat actors. The Stuxnet operation ^[7], for example, used four zero-day (previously unknown vulnerability) exploits against the centrifuge SCADA system of the Iranian uranium enrichment facility at Natanz. The covert nature of Stuxnet meant that the scientists at the facility could not explain what caused the enrichment to fail. Muti and Tajer suggest that this undermined the trust the Iranian government placed in the abilities of the scientists.

In contrast, overt CO allows a state-supported threat actor to demonstrate their capabilities as a deterrent towards potential adversaries. The report speculates that in war, destructive CO against the SCADA systems of CNI (energy infrastructure, transport networks, hospitals, etc.) might result in catastrophic effects, e.g., significant loss of life. However, the technical complexity and the substantial resources required by them mean that, at present, such operations remain the preserve of state-supported threat actors.

The report also describes how nations conduct CO to augment traditional military operations. The authors cite a 2007 Israeli bombing raid, Operation Orchard, on a Syrian nuclear reactor site, to illustrate the vulnerability of military command and control networks. In this instance, the exploitation of the Syrian air defense information network and the subsequent creation of spoofed traffic allowed the free passage of the Israeli aircraft to and from their target ^[8]. Another example occurred during the Russo-Georgian conflict in 2008. Here, Russia conducted low-level CO against web-based financial and governmental services in Georgia prior to the launch of a ground offensive. The operation caused significant disruption to the lives of Georgian citizens and affected the ability of the government to coordinate a response.

Like the Georgian experience, Estonia fell victim to a Distributed Denial of Service (DDoS) CO against the web services of banks and the government. Again, the attack originated from Russia, but on this occasion, the perpetrators stated that they formed part of a government-financed youth collective known as Nashi. The Estonian government was unable to respond in-kind against the Russian government or to invoke the collective defense clause of the North Atlantic Treaty Organization (NATO) (Article 5). In response, Estonia established the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). This organization produced the Tallin Manual on International Law Applicable to Cyber Operations, which proposes that financial support of a threat actor by a state does not constitute

‘overall control’ of the CO conducted by that actor ^[9]. The absence of a normative international framework that addresses the ambiguity that exists in the relationship between states and state-sponsored, threat actors, creates opportunities for CO to occur without the risk of proportionate retaliation.

In their report, Muti and Tajer use the example of China’s efforts in 2013 to disrupt an investigation by the *New York Times* into China’s Prime Minister to illustrate how threat actors seek to control public perception. Analysis by the cybersecurity firm Mandiant ^[10] described how spear phishing e-mails sent to *New York Times* employees contained malicious attachments which, once opened, provided remote backdoor access to their work computers. To disguise the source of the activity, the operation was conducted through compromised proxy hosts in the United States. Once into the system, they escalated their user account privilege to pivot laterally onto other hosts on the network where they exfiltrated sensitive information. This process of compromise-persist-escalate-pivot-compromise forms a standard lifecycle for CO referred to in the cybersecurity community as Advanced Persistent Threat (APT) ^[11].

One area Muti and Tajer failed to illustrate is the internal threat. The unauthorized public disclosure by Edward Snowden of 1.5 million documents demonstrates the potential damage that can be caused by trusted users. A report by the United States House of Representatives referred to the leak of classified information by the former National Security Agency contractor as “the most damaging [...] in history” ^[12].

2.3 Power-laws in cyber-operations

In his article, *How Power-Laws Re-Write the Rules of Cyber Warfare*, Bibighaus describes the fundamental assumption that exists amongst strategic thinkers that, in warfare, Armed Forces shall operate in environments defined by Gaussian randomness ^[13]. Instead, the author argues that in CO, a different type of randomness, governed by Power-Law distribution, exists.

In Gaussian random environments such as the physical world, the factor by which events deviate from the norm is low. Bibighaus cites the example of human height; where the tallest man alive stands at 8’3”, 1.5 times taller than the average. In Power-Law random environments such as personal wealth, a handful of events occur that deviate by a massive factor from the norm. For instance, the author compares the wealth of Bill Gates to that of the average person. The philosopher Nicholas Taleb describes the occurrence of these rare but powerful events as Black Swans. Bibighaus notes that Power-Law distributions follow the Pareto principle, whereby 80% of the impact derives from 20% of the causes ^[14].

In CO, Power-Law randomness manifests itself in several ways. For example, while the vast majority of malicious exploits (or ‘cyber-weapons’) created pose little or no threat, a few are highly damaging. Bibighaus highlights how a single virus, Conficker.B, infected millions of systems as evidence to that effect. Related to this, the author describes how the Power-Law distribution applies to the number of requests made by programs to software libraries. Programs depend on the integrity of these libraries. When threat actors exploit a major software library, large numbers of programs become vulnerable.

The article describes how these rare but powerful exploits require a cyber warrior of exceptional talent to create them. From this, Bibighaus stresses that talent rather than the mass of numbers serves as the primary measure of power in CO. Therefore, the recruitment and retention of gifted ‘cyber warriors,’ and the fundamental requirement for quality over quantity presents an additional factor for policy-makers to consider.

3. APPROACHES TO CYBER-OPERATIONS

3.1 United States

The 2015 DoD cyber strategy sets out the activities that the US armed forces shall undertake to develop a coherent CO capability ^[15]. The DoD defines cyberspace as an operational sub-domain within the information environment, formed of technology infrastructures and data ^[16]. The allocation of ‘domain’ status to cyberspace (alongside maritime, land, air, and space) serves a bureaucratic purpose to ensure that CO receives sufficient financial and material support.

The strategy calls for a national endeavor to defend against the CO of adversarial threat actors. To achieve this, the DoD lists five strategic goals: force readiness, information assurance, defensive operations, offensive operations, and deterrence. A 6,200 strong ‘Cyber Mission Force (CMF)’ shall deliver these goals. The CMF is comprised of 133 teams and is subdivided into the ‘Combat Mission Force’ (CO in support of operations), ‘National Mission Force’ (to counter significant cyber threats) and ‘Cyber Protection Force’ (to defend against day-to-day cyber threats). The DoD aims to establish a capability to model and simulate CO, enabling a regular pattern of network defense exercises to take place. This serves to address the need to train and prepare those individuals involved in CO and prevents the skill-fade that occurs after periods of inaction. Furthermore, the establishment of viable CO career paths shall help retain talented personnel.

The strategy discusses the need to learn from the experience of the private sector, a body that accounts for more than 90% of US network infrastructure. Commercial Computer Emergency Response Teams (CERTs) have found that continuous defensive CO can have psychological effects on the individuals involved, including post-traumatic stress ^[17]. DoD exchange programs with private companies and the employment of part-time, cyber reservists helps develop a better understanding of such effects and fosters institutional

resilience. To further reduce the burden on the defender, the strategy calls for penetration testing of internal networks to identify vulnerabilities before adversaries and introducing automated patch management. Moreover, the strategy mentions the need to deter potential threat actors through statements of policy and demonstrations of powerful intrusion detection, attribution ^[18], and retaliation capabilities.

3.2 China and Russia

The information warfare doctrinal approach of China and Russia differs from the US. In a 2009 paper, Timothy Thomas sets out these how these countries operate in cyberspace ^[19]. China's doctrine makes little reference to the 'cyber' prefix, preferring to consider computer systems and networks as a target for informationization. China's approach to informationization (and by extension CO) involves the pre-emptive use of stratagems, methods, and technology to control networks. The goal is to achieve an information advantage over the cognitive process of an adversary. The reference to pre-emptive action acknowledges the fact that CO takes time (sometimes several years) to prepare, but are required to deliver sudden, intended effect. Chinese doctrine suggests the use of CO to compromise (but not control) networks should occur in peacetime in response to strategic threat assessments. To achieve this, China must pre-emptively recruit talented individuals and establish links with the private sector. However, the Chinese military aims to avoid becoming too dependent on computer systems and information networks. The doctrine notes that Occidental (Western) armed forces rely heavily on solving problems with fragile technical solutions. A better approach, the Chinese suggest, is to focus on building cognitive resilience.

Russia also prefers to use the term informationization to describe CO. Russian doctrine on the subject states the purpose of informationization/CO as being to deliver reflexive control over an adversary. Reflexive control refers to the exploitation of weaknesses in a cognitive system to predict or influence decisions. The doctrine categorizes weakness into two types; information-technical and information-psychological. One example of information-psychological weakness might be the personal characteristics of a military commander (experience, belief, knowledge, etc.) that inform their decisions. Information-technical refers to the hardware, software, and data that facilitate and contribute to a cognitive process. Thomas cites the Russian military strategist Col. Leonenko ^[20] to suggest that the absence of intuition in computer cognition makes them vulnerable to reflexive control. A piece of software cannot tell, for instance, the difference between normal data and deceptive data.

Moreover, Leonenko argues that the introduction of semi- and fully autonomous systems represents a dangerous evolution in military capability. Autonomous cognition requires environments of certainty. Commanders trust these systems to make independent decisions, yet they cannot respond to previously unseen circumstances. Schneier proposes that network defense represents one area where trust in automated responses has been misplaced ^[21].

3.3 *United Kingdom (Royal Navy)*

The Cyber primer ^[22] forms the primary source of published UK doctrine on CO. The document provides a high-level overview of cyberspace and introduces the way the UK plans to conduct CO. In line with the layered domain model, the UK MOD approaches cyberspace as an operating environment across the physical, virtual, and cognitive domains that is formed of information networks and data. However, the definition fails to acknowledge the human component of cyberspace, on which all non-autonomous information networks depend. Terminology serves a vital role in the interpretation of doctrine. Failure to acknowledge the role of people (unlike the Russians) shall misguide commanders about the potential reach of CO.

The MOD considers CO as taking place in the near, mid, and far spaces of cyberspace. Near describes the information networks under the direct control and assurance of the Armed Forces. The mid-space exists in the networks of friendly third-parties (allies, other government departments, etc.). Those networks that are outside the control and assurance of the MOD or friendly third-parties are described as far operating spaces.

Within these spaces, the Armed Forces conduct defensive and offensive CO, alongside cyber intelligence, surveillance, and reconnaissance, and operational preparation of the environment. The UK doctrine highlights the need for the incorporation of these operations into wider military planning, to provide commanders with a ‘full spectrum’ targeting capability. The doctrine acknowledges the limitations of CO to affect the operational and tactical levels of conflict. Access to adversarial information networks often takes years to achieve, which means that offensive CO shall take place before any military activity, delivering an advantageous effect at the onset (e.g., Israeli bombing of Syrian reactor).

The MOD manages the resources with which to conduct CO centrally through the Joint Forces Cyber Group. Within the group sits Joint Cyber Unit (JCU) Cheltenham and JCU Corsham, deliver offensive and defensive CO capability respectively. The technically complex nature of offensive CO means that the mandate to conduct them is held at the JCU level. Nonetheless, the Royal Navy cyber strategy ^[23] describes the inherent advantages regarding mobility, persistence, and proximity to target that maritime platforms offer. In a sense, the Royal Navy provides a near cyberspace environment through which to conduct CO against other maritime platforms and littoral information networks. For example, warships and submarines equipped with powerful directional antennas will be able to intercept wireless internet traffic or exploit access points in coastal areas.

While JCU Corsham holds overall authority for defensive CO, the responsibility to defend specific assets exists at the single service level. The Royal Navy faces several unique challenges in this area. Naval platforms depend on a multitude of networked systems, including communication, navigation, propulsion, life-support (water, waste, etc.), and weapons. Vulnerabilities in these systems pose a significant risk to operational effectiveness.

Moreover, the technical limitations around the transfer of data over long distances means that naval platforms depend on low bandwidth communication (measured in kB/s). This causes problems for the distribution of vulnerability patches and software updates to deployed warships and submarines. The lack of bandwidth also means that the Royal Navy must employ network monitoring and active defense capabilities at the platform (local) level. Warships and submarines must respond to and recover from the initial effects of CO without external support. To address this challenge, the Royal Navy introduced Cyber Protection Teams (CPTs). Three levels of Royal Navy CPTs exist underneath JCU Corsham (Figure 1). Each platform shall deploy with at least a Level One CPT in the role of a system administrator to protect against day-to-day cyber threats ^[24]. Level Two CPTs shall deploy onboard larger platforms (aircraft carriers, landing ships) to provide increased protection (e.g., active network monitoring). The CDOC is the central coordinator for Royal Navy defensive CO and offers a deployable Level Three (expert) capability when required.

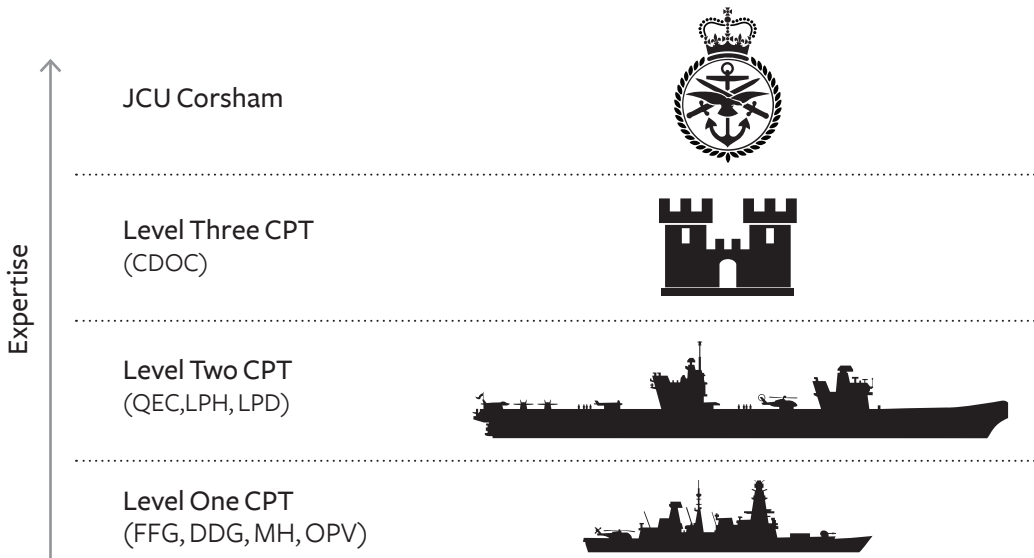


Figure 1. Hierarchy of Royal Navy Defensive CO

Members of the CDOC stress that their primary mission is to remotely track and manage vulnerabilities in the systems of deployed units. However, a significant issue faced by the CDOC is the lack of commercial openness inherent in traditional military network procurement which drives the emergence of Vendor ‘lock-in’^[25]. Failure to escape technological lock-in results in the use of legacy systems, with known vulnerabilities, to deliver operational capability. Moreover, contractual arrangements mean the CDOC is unable to perform penetration testing against these systems or make modifications to mitigate vulnerabilities.

4. CYBER RECRUITMENT AND TRAINING

Personnel employed in the CDOC come from the full-time trained strength of the Royal Navy’s Information Warfare Division. Separate to this, the establishment of the Maritime Cyber Reserve in 2014^[26] provided the Royal Navy with a means by which to recruit talented individuals from the private sector. Moreover, the Royal Navy recruits a small proportion of civilian maritime cyber reservists who, in normal circumstances, would fail to meet the physical entry requirements. Maritime cyber reservists augment the activities of the JCUs and provide the workforce for the Royal Navy Reserve Cyber Unit. The specialist nature of the work undertaken by cyber reservists necessitates that their career advancement occurs within the confines of their respective unit and that promotion is based on merit rather than the length of service. The MOD uses an aptitude test, together with a competency framework of four levels (Awareness, Practitioner, Senior Practitioner, and Expert) to measure technical skill and to allocate cyber roles. For example, members of Level One CPTs require at least an Awareness competency. To achieve the Awareness and Practitioner competencies, individuals must attend a series of technical training courses. The role of these courses is important in developing a skill set that applies to real-world cyber-security. As Conklin et al., point out, graduates of cyber-related degree programs often lack the practical skills from real-world experience required for such activity^[27].

The ‘Advanced Course in Engineering (Information Assurance)’ established by academics^[28] at the United States Air Force Research Laboratory, provides an excellent example of an intensive, technical training program for armed forces personnel in cyber roles. The course takes place over an eleven-week period and exposes participants to a significant number of the concepts that apply to CO. Each week individuals on the course must write a thirty to forty-page report on a subject introduced by experts from across defense, academia, and industry. In parallel, the participants are divided into two teams, and each team is expected to apply the lessons they learn to conduct CO against the other. The course culminates in a large-scale East vs. West Capture the Flag (CTF) exercise, involving cyber-physical elements such as drones and rovers.

The CTF format serves as the basis for most system-on-system CO training activities. Cowan et al. provide an overview of the normal components of a CTF exercise ^[29]. CTF consists of at least two networked teams in competition against one another. Each team owns a server with known vulnerabilities, on which resides a data file (the flag). To score points, a team must compromise the server of an opponent and replace the flag with their own. At the same time, the team must defend their network and prevent their flag from being compromised. An independent server monitors the network and scores teams for successful offensive and defensive CO. To encourage teams to think cleverly about their actions, the score server places a fine on bandwidth usage. While not directly applicable to maritime CO (i.e., there is no attempt to achieve “reflexive control”), CTF exercises provide technical experience and help participants understand the pressures that come with CO.

5. KEY RECOMMENDATIONS

The Royal Navy should:

- ◆ Update doctrine definitions of cyberspace to recognize the human component.
- ◆ Introduce a talent-scout model of recruitment (‘tap-on-the shoulder’) to find individuals with exceptional skills and to create the perception of the Royal Navy as an elite place to work.
- ◆ Establish viable career paths for regular, full-time personnel who wish to work in cyber roles.
- ◆ Procure mechanisms to reduce the operational and tactical effects of CO in times of conflict (e.g., distributed software-defined networking, and virtualization).
- ◆ Ensure those employed to monitor the information networks on platforms understand how to respond and recover from CO locally.
- ◆ Work with commercial CERTs to understand the psychological risks to those who conduct high-intensity defensive CO.
- ◆ Utilize simulations and models of platform networks to train personnel involved in defensive and offensive CO. Work with the cyber-security community to introduce CTF elements into training exercises like INFORMATION WARRIOR and ‘Flag Officer Sea Training’.
- ◆ Approach the introduction of autonomous and artificially intelligent systems ^[30] with caution, and in acknowledgement of their unsuitability to environments of uncertainty.

6. CONCLUSION

This paper illustrates many of the risks and opportunities faced by the Royal Navy in cyberspace. A diverse range of threat actors works to collect and control information by exploiting vulnerabilities that exist in the networks and systems that form cyberspace. For military organizations, the harm caused by these activities often reaches beyond the intended victim network or system, damaging operational and strategic functions. Defense doctrine serves a crucial role in communicating these dangers to planners and decision-makers to help formulate response mechanisms and mitigation strategies. The Royal Navy approach to defensive CO focuses on the need to protect platforms at the local level. CPTs deployed on board ships and submarines aim to mitigate day-to-day threats, while expert CPTs are prepared to respond to significant incidents. The US DoD strategy highlights the importance of cooperation with private sector cyber-security groups who have extensive experience in defensive CO.

Offensive CO, on the other hand, present opportunities for armed forces to augment traditional military activities. The Russian and Chinese literature on the subject discusses how informationization (offensive CO) targets the cognitive functions (autonomous and human) of an adversary to control their decisions. The Royal Navy appreciates the potential of such operations, especially when conducted by persistent and mobile maritime platforms. The service must develop understanding and experience in this area through regular CTF-type exercises.

Overall, the Royal Navy has made good progress in establishing the organizational structures and concepts with which to conduct CO. The naval service must now build the confidence to survive, operate and fight in cyberspace. 🛡️

NOTES

1. D. Ormrod, and B. Turnbull, “The cyber conceptual framework for developing military doctrine”, *Journal of Military and Strategic Studies* Volume 16, Issue 3, May 31, 2016, 270-298.
2. Development, Concepts and Doctrine Centre, “Cyber primer (second edition)”, Joint Doctrine Publication, Ministry of Defence 2016, [Technical Report], <https://www.gov.uk/government/publications/cyber-primer>.
3. HM Government, “National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom”, November 2015. [Technical Report], <https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015>.
4. I. Driva, “Maritime Cyber Security for Navigation and Control Systems”, MSc Dissertation, School of Electronics and Computer Science University of Southampton, September 2, 2016.
5. VERTIC, A. Muti, and K. Tajer, with L. Macfaul, “Cyberspace: An assessment of current threats, real consequences and potential solutions”, The Remote Control Project, October 2014, [Technical Report], <http://remotecontrolproject.org/publications/cyberspace-an-assessment-of-current-threats-real-consequences-and-potential-solutions/>.
6. M. D. Cavely, “Cyber-Security and threat politics: US efforts to secure the information age“, Routledge, Abingdon, 2008.
7. R. Langer with G. McGraw, “An Interview with Ralph Langner“, Silver Bullet Podcasts, Show 059, Cigital, February 25, 2011, <https://www.cigital.com/podcasts/show-059/>.
8. D. Fulghum and R. Wall, “Israel Shows Electronic Prowess: Attack on Syria shows Israel is master of the high-tech battle”, *Aviation Week Intelligence Network*, November 26, 2007, <http://aviationweek.com/awin/israel-shows-electronic-prowess>.
9. M. N. Schmitt, “Tallinn manual on the international law applicable to cyber warfare”, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, Cambridge, 2013.
10. N. Perloth, “Hackers in China Attacked The Times for Last 4 Months”, *NY Times*, January 30, 2013, <https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>.
11. Mandiant Intelligence Center, “Apt1: Exposing one of China’s cyber espionage units.”, Mandiant, 2013, [Technical Report], Available at <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.
12. Permanent Select Committee on Intelligence, “(U) Review of the unauthorized disclosures of former National Security Agency contractor Edward Snowden”, United States House of Representatives, September 15, 2016, [Technical Report], https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf.
13. D L. Bibighaus, “How power-laws re-write the rules of cyber warfare”, *Journal of Strategic Security*, Volume 8, Issue 4, Henley-Putnam University, 2015, 39-52.
- 14 N N. Taleb, “The black swan: The impact of the highly improbable“, (The Incerto Collection), Random House and Penguin, London, 2007.
- 15 A. Carter, “The DOD cyber strategy.”, Department of Defense, Washington D C, 2015, [Technical Report], https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
- 16 Defense Technical Information Center, “Joint Publication 3-12(R): Cyberspace Operations”, Joint Electronic Library, June 8, 2018, [Technical Report], http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
- 17 V. Pegueros, “DocuSign CISO Discusses The Human Element of Incident Response Security”, *Current Podcasts Show* 105, 25 February 2011, https://traffic.libsyn.com/insight/Vanessa_Pegueros_-_Human_Element_of_IR_-_2-28-2017.mp3.
- 18 Office of Public Affairs, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”, Department of Justice, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.
19. T. Thomas, edited by F. Kramer, et al, “Nation-state cyber strategies: Examples from China and Russia.”, *Cyberpower and National Security*, University of Nebraska Press, 2009, 465-488.
20. S. Leonenko, “Refleksivnoe upravlenie protivnikom [Reflexive control of the enemy]”, *Armeiskii sbornik (Army Collection)*, Issue 8, 1995, 28.
21. Schneier B, “Crypto-Gram“, *Schneier on Security*, April 15, 2017, <https://www.schneier.com/crypto-gram/archives/2017/0415.html>.

NOTES

22. Development, Concepts and Doctrine Centre, “Cyber primer (second edition)”, Joint Doctrine Publication Ministry of Defence, 2016, [Technical Report], <https://www.gov.uk/government/publications/cyber-primer>.
23. Royal Navy, “Cyber Strategy”, Navy Command Headquarters, 2014.
24. RNTM 165/16, “Cyber Essentials: Level One Cyber Protection for the Naval Service”, Royal Navy, 2016.
25. J. Connah, A. Solomon, J. McInnes, and O. Worthington, “Openness in military systems”, Defence Science and Technology Laboratory (DSTL), 2012 Military Communications and Information Systems Conference (MCC), Gdansk, October 8-9, 2012.
26. CMRTM 24/14, “Maritime Cyber Reserves and the Formation of the RNR Cyber Unit”, Commander Maritime Reserves, 2014.
27. A. Conklin, R E. Cline, and T. Roosa, “Re-engineering cybersecurity education in the US: An analysis of the critical factors”, 2014 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, January 2014, 6-9.
28. Jabbour K and Older S, “The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-Security Leaders”, Syracuse University, 2004.
29. C. Cowan, S. Arnold, S. Beattie, C. Wright, and J. Viega, “Defcon capture the flag: Defending vulnerable code from intense attack.”, DARPA Information Survivability Conference and Exposition, 2003 Proceedings, Volume 1, IEEE, Washington D C, April 2003, 22-24.
30. A. Johnston, “Innovation Challenge - Artificial Intelligence in Royal Navy Warships”, techUK, London, October 17, 2016, <https://www.techuk.org/events/briefing/item/9400-innovation-challenge-artificial-intelligence-in-royal-navy-warships>.

Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks

Dr. Alexander Kott

ABSTRACT

Intelligent autonomous agents will be widely present on the battlefield of the future. The proliferation of intelligent agents is the emerging reality of warfare, and they will form an ever-growing fraction of total military assets. By necessity, intelligent autonomous cyber defense agents are likely to become primary cyber fighters on the future battlefield. Initial explorations have identified the key functions, components and their interactions for a potential reference architecture of such an agent. However, it is beyond the current state of Artificial Intelligence (AI) to support an agent that could operate intelligently in an environment as complex as the real battlefield. A number of difficult challenges are yet to be resolved. At the same time, a growing body of research in Government and academia demonstrates promising steps towards overcoming some of the challenges. The industry is beginning to embrace approaches that may contribute to technologies of autonomous intelligent agents for the cyber defense of the Army networks.

A cyber defense agent among other intelligent things

The landscape of possible AI applications in the military seems enormously broad. However, if we were to seek the primary types of “intelligent things” (i.e., embodiments of AI in user-relevant capabilities) most directly relevant to the future of ground warfare, we may find a rather small number of such types. In the following, I offer my vision of a pragmatic taxonomy of such intelligent entities, as they may appear on the battlefield of the mid- to long-term future (perhaps in years 2035-2050). This taxonomy is not exclusive, but it does cover a large fraction of functions where AI is likely to have impact on ground combat. In this article, I intend to focus on only one of these types—the cyber defense agent—but it helps to introduce it as a member of a broader family of intelligent agents.

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



Alexander Kott earned his PhD in Mechanical Engineering from the University of Pittsburgh, Pittsburgh, PA, in 1989, where he researched AI approaches to invention of complex systems.

He serves as the US Army Research Laboratory's (ARL) Chief Scientist in Adelphi MD. In this role he provides leadership in development of ARL's technical strategy, maintaining technical quality of ARL research, and representing ARL to external technical community. Between 2009 and 2016, he was the Chief, Network Science Division, Computational and Information Sciences Directorate, ARL, responsible for fundamental research and applied development in network science and science for cyber defense. In 2003-2008, he served as a Defense Advanced Research Programs Agency (DARPA) Program Manager. His earlier positions included Director of R&D at Carnegie Group, Pittsburgh, PA. There, his work focused on novel information technology approaches, such as Artificial Intelligence, to complex problems in engineering design, and planning and control in manufacturing, telecommunications and aviation industries.

Dr. Kott received the Secretary of Defense Exceptional Public Service Award, in October 2008. He published over 100 technical papers and served as the co-author and primary editor of over ten books.

Intelligent off-road ground mover

This is a physical vehicle, a robot—whether it is legged, wheeled or tracked—intended for moving other intelligent entities (including Soldiers), supplies, munitions and weapon systems around the battlefield. Today such vehicles are largely tele operated at low speeds or can drive autonomously on well-ordered roads, or follow the leader on unimproved roads (Machi 2018).

The high lethality and dispersion of the future battlefield will make the wide use of such movers a necessity. The mover will be capable of fast and tactically appropriate movements in complex terrain, such as rough, heavy forests, mountains, and urban rubble, and possibly even climbing over obstacles using limbs. It will self-manage its trips to charging/refueling stations and self-recharging, self-right when overturned, and autonomously load and unload. It will plan fairly complex tasks given a general intent by the Soldier, and collaborate with other intelligent agents.

Intelligent munition

These physical entities will approach and defeat an adversary's asset, either by kinetic or other means. Some will resemble today's ancestors like guided artillery shells, fire-and-forget munitions, and weaponized unmanned aerial vehicles (UAVs).

Future intelligent munitions will be necessitated partly by the proliferation of adversary autonomous systems. The bulk of these munitions will target the adversary munitions and information collectors. They will likely be able to conduct autonomous scene assessment and (moving) target recognition in a cluttered ground environment, as well as to recognize adversary countermeasures and to perform aggressive maneuvers to avoid them. Some will be able to autonomously plan a nap-of-the-earth flight, multi-munition collaboration to defeat hard targets,

and collaborative allocation and pursuit of multiple authorized targets. Others will be defensive in nature such as the autonomous active protection systems (Freedberg 2016). When such intelligent munitions are used by the US, they will comply with strong constraints on autonomous and semi-autonomous weapon systems established by the US Department of Defense (Hall 2017). When the munitions are used by other countries, it is hard to predict what constraints they may comply with, if at all.

Intelligent information collector: What encourages innovation?

Today's UAVs and UGVs collect sensor information while being largely tele operated and following predefined waypoints. Humans make detailed decisions about what data is to be collected, when, where, and how.

Even today, management of collection assets is burdensome for Soldiers. With the ever-increasing number of such assets, future intelligent collectors will have to become broadly autonomous in formulating their paths and collection plans, based on the mission and intent provided by Soldiers. The plans could be even autonomously defined in collaboration with other collectors and based on gaps in available information. Many of them will be small, micro-autonomous systems (Piekarski et al., 2016), that will fly, perch, and crawl in a way that minimizes their detection by the adversary. Some will be capable of fast nap-of-the-earth movements through forests and urban terrain. They will perform continuous adversarial reasoning to understand the adversary and to minimize the probability of detection by the adversary. They will plan and manage their launch and recovery, recharging and maintenance, and in general try to minimize their burden on the Soldiers.

Intelligent information integrator and interpreter

Today's AI models can perform functions like imagery fusion and automated detection of certain targets and patterns of activity in images and video yet, much of the collected information cannot be properly processed and interpreted. As the volume of available, collected information continues to increase, the situation will steadily get more challenging.

In the future, information integrator agents will be able to use multiple, highly dissimilar types of information to perform continuous recognition and interpretation of enemy and friendly activities on broad battlefield scale, along with a projection of upcoming adversary activities. They will be able to collaborate in a distributed operation and communicate with Soldiers by explaining the basis for their findings and pointing out the potential implications of the findings. They will keep up with evolving conditions and adversaries by rapid learning from a small number of examples. They will be capable of adversarial reasoning (inferring the adversaries plans) and mindful of deception, e.g., the challenge of adversarial learning (Papernot et al., 2016).

Intelligent COA generator and monitor

These virtual agents will have to be far more autonomous than today's versions that support human-driven planning mainly as computerized drawing boards and maps and templates. The future battles, with high numbers of robotic assets, will acquire greater tempo and will demand detailed planning and agile execution not only for Soldiers but also the far more numerous intelligent agents. The future agents will perform largely autonomous—but collaborating with Soldiers and other intelligent agents as appropriate—preparation of plans for robotic collectors and asset movers and ongoing dynamic management of a fast-moving, robotic-heavy battle at scale with limited guidance from humans. Such an agent will operate in a distributed fashion, will collaborate closely with the intelligent information integration agents, and will conduct continuous wargaming to assess a range of alternative plans.

Intelligent network management agent

Today's network management tools are largely limited to centralized network controllers that display information and allow engineers to push configuration changes, often with the help of specialized scripting languages and libraries of scripts. Even today, this approach is hardly adequate for managing dynamic tactical networks, and the coming decades will see networks with ever-growing complexity, diversity and fast changes in operations. Future network management agents will operate collaboratively to ensure self-forming and self-healing networks that respond to complex, large-scale disruptions, including the ability to anticipate and proactively adapt to adversarial actions. They will continually perform autonomous identification and modeling of the network, detect anomalies and perform configuration and topological changes, and manage trust.

Intelligent cyber defense agent

Finally, the primary topic of this article: the intelligent cyber defense agent. Today's related capabilities include firewalls, intrusion detection and alerting, and scripted removal of known malware.

In the future, just like physical robots, cyber agents will be employed in a range of roles. Some will protect communications and information (Stytz et al., 2005) or will fact-check, filter and fuse information for cyber situational awareness (Kott et al., 2014). Others will defend electronic devices from effects of electronic warfare. These defensive actions might include the creation of informational or electromagnetic deceptions or camouflage. An intelligent cyber agent will be capable of planning and execution of complex multi-step activities for defeating or degrading sophisticated adversary malware, with anticipation and minimization of resulting side effects. It will be capable of adversarial reasoning to avoid detection and defeat by adversary agents and collaborate on planning and actions with friendly agents. In the remainder of the article, I will talk in more detail about the functions and capabilities of such agents.

The cyber agent is exceptionally important among the examples of agents I listed above. None of the other agents can directly help the cyber agent survive on the battlefield of the future. At the same time, none of the other agents can themselves survive without the protection of the cyber agent.

In a major conflict with a peer competitor, the friendly tactical networks will face a strongly contested environment. The sophisticated adversary will continually attack the networks and devices with cyber and electromagnetic technologies. Its capable malware – the adversary cyber agents – will, in some cases, penetrate and operate on the friendly devices. In other words, all intelligent agents I have described will be targets of cyberattacks. The potential that a significant number of such agents will participate on the future battlefield makes cyberattacks exceptionally beneficial to the adversary, if they are successful and not effectively opposed.

Today's reliance on human cyber defenders will be untenable in the future. The proliferation of intelligent agents is the emerging reality of warfare, and they will form an ever-growing fraction of total military assets (Scharre 2014). The sheer quantity of targetable friendly agents, the complexity and diversity of the overall network of entities and events, the fast tempo of robotic-heavy battle, the difficulties of centralized defense in a communications-contested environment, the relative scarcity of human Soldiers in highly dispersed operations, and the high cognitive load imposed on them by activities other than cyber defense—all make intelligent, autonomous cyber defense agent a necessity on the battlefield of the future.

In the remainder of this article, I will describe the possible functions and architecture of an intelligent autonomous cyber defense (based mainly on (Kott et al., 2018)), and the limitations of today's AI (following mainly (Kott 2018)) that would need to be overcome in order to make such agents feasible and effective, and offer a few examples of today's efforts aimed at developing such agents.

Desired capabilities of an intelligent cyber defense agent

In this section, I mainly follow the documents produced by a NATO Science and Technology Organization's research group on "Intelligent Autonomous Agents for Cyber Defense and Resilience," which I happen to chair. The group's objective is to help accelerate the development and transition to practical use of such intelligent agents by producing a reference architecture and a technical roadmap (Kott et al., 2018; Theron et al., 2018).

To limit the scope of the discussion, consider a single autonomous platform, such as an intelligent ground mover or an intelligent munition (such as I described earlier) with one or more computers residing on the platform, connected to sensors and actuators. Each computer contributes considerably to the operation of the platform or systems installed on the platform. One or more computers are assumed to have been compromised by the adversary malware, where the compromise is either established as a fact or is suspected.

Due to the contested nature of the communications environment (e.g., the adversary is jamming the communications, or radio silence is required to avoid detection by the adversary), communications between the vehicle and other elements of the friendly force are limited and intermittent at best. Given the constraints on communications, conventional centralized cyber defense (i.e., an architecture where local sensors send cyber-relevant information to a central location where highly capable cyber defense systems and human analysts detect the presence of malware and initiate corrective actions remotely) is often infeasible. It is also unrealistic to expect that Soldiers, even if they have direct access to the autonomous vehicle, will have the necessary skills or time available to perform cyber defense functions concerning the vehicle.

Therefore, the cyber defense of such a platform, including its computing devices, will be performed by an intelligent, autonomous agent. The agent (or multiple agents per platform) will stealthily monitor the networks, detect the adversary agents while remaining concealed, and then destroy or degrade the adversary malware. Provisions are made to enable a remote or local human controller to fully observe, direct, and modify the actions of the agent. However, it is recognized that human control will often be impossible. Similarly, provisions are made for the agent to collaborate with agents residing on other vehicles; however, in most cases, because the communications are impaired or observed by the adversary, the agent operates alone.

To fight the adversary malware deployed on the friendly computer, the agent often has to take destructive actions, such as deleting or quarantining certain malware. Such destructive actions are carefully controlled by the appropriate rules of engagement and are allowed only on the computer where the agent resides. The actions of the agent, in general, cannot be guaranteed to preserve the availability or integrity of the functions and data of friendly computers. There is a risk that an action of the agent will “break” the friendly computer, disable important friendly software, or corrupt or delete important data. Developers of the agent will attempt to design its actions and planning capability to minimize the risk. This risk, in a military environment, has to be balanced against the death or destruction caused by the adversary if the agent’s action is not taken.

The adversary malware, specifically, its capabilities and tactics, techniques, and procedures (TTPs) evolve rapidly. Therefore, the agent will be capable of autonomous learning. In case the adversary malware knows that the agent exists and is likely to be present on the computer, the adversary malware seeks to find and destroy the agent. Therefore, the agent will possess techniques and mechanisms for maintaining a certain degree of stealth, camouflage, and concealment. More generally, the agent takes measures that reduce the probability that the adversary malware will detect the agent. The agent is mindful of the need to exercise self-preservation and self-defense.

It is assumed here that the agent resides on a computer where it was originally installed by a human controller or authorized process. It is possible to envision that an agent may move (or move a replica of itself) to another computer. However, such propagation is assumed to occur only under exceptional and well-specified conditions and takes place only within a friendly network—from one friendly computer to another friendly computer.

This brings to mind the controversy about “good viruses.” Such viruses have been proposed and dismissed earlier (Muttik 2016). These criticisms do not apply here. This agent is not a virus, because it does not propagate except under explicit conditions within authorized and cooperative nodes. It is also used only in military environments, where most of the concerns about ‘good viruses’ do not apply.

The architecture of the agent, partly derived from the widely accepted model of Russell and Norvig (2009), is assumed to include the functional components shown in Fig. 1.

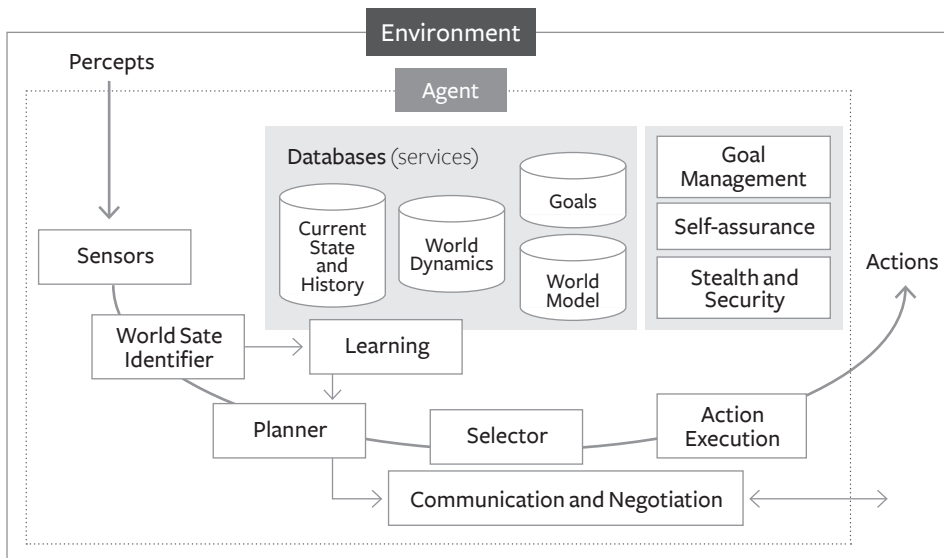


Figure 1. Functional Architecture of an Autonomous Intelligent Cyber Agent (Kott et al 2018).

AI will be challenged by the complex cyber battlefield

An intelligent cyber agent will have to operate on a highly complex and dynamic battlefield. Consider Fig. 2 that depicts an environment in which a highly-dispersed team of human Soldiers and intelligent agents (including but not limited to physical robots) is facing physical and cyber threats. The agents must be effective, in this unstructured, unstable, rapidly changing, chaotic, adversarial environments; they must learn in real-time, under extreme time constraints, using only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive.



Figure 2. An intelligent cyber agent will operate in extremely complex, challenging environment: unstructured, unstable, rapidly changing, chaotic, adversarial and deceptive.

Clearly, it is beyond the current state of AI to operate intelligently in such an environment—physical or cyber—and with such demands. While the use of AI for battlefield tasks has been explored on multiple occasions, e.g., (Rasch et al., 2002), and AI makes things individually and collectively more intelligent, it also makes the battlefield more difficult to understand and manage. Agents and Soldiers have to face a much more complex, and unpredictable world where intelligent agents have a mind of their own and perform actions that may appear inexplicable to the humans. Direct control of such intelligent agents by humans becomes impossible or limited to cases of whether to take specific destructive action.

An intelligent cyber agent will need to deal with a world where sheer number and diversity of cyber objects will be enormous. The number of connected computing devices, for example within a future Army brigade, is likely to be several orders of magnitude greater than in current practice. This, however, is just the beginning. Consider that computing devices belonging to such a brigade will inevitably interact—willingly or unwillingly—with devices owned and operated by other parties, such as those of the adversary or owned by the surrounding civilian population. If the brigade operates in a large city, where each apartment building can contain thousands of devices, the overall universe of connected

items grows to enormous numbers. A million devices per square kilometer is not an unreasonable expectation.

The above scenario also points to a great diversity of devices within the environment of the intelligent cyber agent. Devices will come from different manufacturers, with different designs, capabilities, and purposes, configured or machine-learned differently, etc. No individual agent will be able to use pre-conceived (pre-programmed, pre-learned, etc.) assumptions about behaviors or performance of other agents or devices it meets on the battlefield. Instead, behaviors and characteristics will have to be learned and updated autonomously and dynamically during the operations. This includes humans, and therefore the behaviors and intents of humans, such as friendly warfighters, adversaries, and civilians and so on will have to be continually learned and inferred.

And yet, Machine Learning (ML), an area that has seen dramatic progress in the last decade, must experience major advances to become relevant to the real battlefield. Learning with a very small number of samples is a necessity in an environment where the adversary and friends change tactics continuously, and the environment itself is highly fluid, rich with details, dynamic and changing rapidly. Furthermore, very few if any of the available samples will be labeled, or at least not in a very helpful manner.

Some samples may be misleading in general, even if unintentionally (e.g., an action succeeds even though an unsuitable action is applied), and the machine learning algorithms will have to make the distinction between relevant and irrelevant, instructive and misleading. Also, some of the samples might be a product of intentional deception by the adversary. In general, issues of Adversarial Learning (Papernot et al., 2016) and Adversarial Reasoning (Kott and McEneaney 2006) are of great importance to ML.

Yet another challenge that is uniquely exacerbated by battlefield conditions are constraints on the available electric power and computing power. Today, most successful AI relies on vast computing and electrical power resources including cloud-computing reach-back when necessary. The battlefield AI, on the other hand, must operate within the constraints of edge devices. This means that computer processors where the intelligent cyber agent resides must be relatively lights and small, and as frugal as possible in the use of electrical power. One might suggest that a way to overcome such limitations on computing resources available directly on the battlefield would be to offload the computations via wireless communications to a powerful computing resource located outside of the battlefield. Unfortunately, this is not a viable solution, because the adversary's inevitable interference with friendly networks will limit the opportunities for the use of reach-back computational resources.

Current efforts towards development of intelligent cyber agents

In spite of the profound challenges, foundational capabilities are gradually emerging that would contribute to an autonomous intelligent cyber defense agent I describe here.

For example, I already mentioned the NATO research group (initiated in 2016 under the title IST-152-RTG “Intelligent Autonomous Agents for Cyber Defense and Resilience.”) The group is in the process of conducting focused technical analysis to produce a first-ever reference architecture and technical roadmap for autonomous cyber defense agents (Kott et al., 2018).

The group’s future plans include the study of use cases that could serve as a reference for the research, as would lead to clarifying the scope, concepts, functionality, and functions’ inputs and outputs of such an intelligent agent. The initially assumed architecture would be refined by drawing further lessons from the case studies. In addition, the group is working to identify and demonstrate selected elements of such capabilities, which are beginning to appear in academic and industrial research.

Based on the analysis of the proposed architecture and available technological foundation, the group is developing a roadmap towards initial yet viable capabilities. The first phase of the roadmap will include the development of knowledge-based planning of actions, the execution functionality, elements of resilient operations under attack, and adaptation of the prototype agent for execution of a small computing device. This phase would culminate in a series of Turing-like experiments that would evaluate the capability of the agent to produce plans of remediating a compromise, as compared to the experienced human cyber defender.

The second phase would focus on adaptive learning, the development of a structured world-model, and mechanisms for dealing with explicitly defined, multiple and potentially conflicting goals. At this stage, the prototype agent should demonstrate the capability, in a few self-learning attempts, to return the defended system to acceptable performance after a significant change in the adversary malware behavior or techniques and procedures.

The third phase would delve into issues of multi-agent collaboration, human interactions, and ensuring both the stealth and trustworthiness of the agent. Cyber-physical challenges may need to be addressed as well. This phase would be completed when the prototype agents can successfully resolve a cyber compromise that could not be handled by any individual agent.

Relevant research in academia and the Army research organizations is growing. Let me mention a few examples. Deployment of an intelligent cyber defense agent on an edge device with limited computational power requires very light yet useful packet analysis capability. Researchers at the US Army Research Laboratory developed such extremely lightweight intrusion detection prototype (Chang et al., 2013) and a similarly lightweight malware traffic classification algorithm that uses continuous machine learning (Ken and Harang 2017). Approaches are also emerging that would enable an intelligent agent to autonomously patch software on a lightweight device once a vulnerability in that software is detected (Azim et al., 2014).


In cases when a cyber agent defends an agent with physical functions, such as an intelligent ground mover, or a collector, detection, and remediation of a cyber-physical attack are particularly important. In that respect, an interesting example is the research at Purdue University (Fei et al., 2018). An autonomous agent was installed on a quadcopter. A series of attacks were then launched by embedding malicious code in the control software and by altering the vehicle's hardware with the specific targeting of sensors, controller, motors, vehicle dynamics, and operating system. Experimental results verified that the agent was capable of both detecting a variety of cyber-physical attacks, while also appropriately taking over the control system in order to recover from such attacks.

Deception and related techniques are among the most effective actions that an intelligent cyber agent can take to defend a system against malware while remaining undetected by the malware and its command and control operators. An example of research in that direction is described in (Asaleh et al., 2017) where an agent performs dynamic analysis of the detected malware and then plans and executes several types of deceptive actions depending on the behavior and intents of the malware. The malware remains unaware that it is being deceived. Similarly, a commercial product from Attivo Networks (Woodard 2017) helps achieve network security by luring, engaging and trapping threats and malware from infected clients and servers in the user network, data center, cloud, and SCADA/ICS network.

Speaking of commercial products, the industry is rapidly growing and evolving a space of products called Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR). These deserve a separate discussion (Gartner 2018). They are clearly driven by some of the same motivations and would depend on some of the same technology advances that I discuss in this article. It is likely, however, that such commercial solutions will continue to rely on assured access to a centralized server or cloud support, and for this reason will prefer to limit the autonomy of the host-based agent.

CONCLUSIONS

Intelligent autonomous agents are a key type of intelligent entities that will be widely present on the battlefield of the future. The proliferation of intelligent agents is the emerging reality of warfare, and they will form an ever-growing fraction of total military assets. By necessity, intelligent autonomous cyber defense agents are likely to become primary cyber fighters on the future battlefield. Indeed, today's reliance on human cyber defenders will be untenable in the future. The reasons include the sheer quantity of targetable friendly agents, the complexity and diversity of the overall network of entities and events, the fast tempo of robotic-heavy battle, the difficulties of centralized defense in a communications-contested environment, the relative scarcity of human Soldiers in the highly dispersed operations, and the high cognitive load imposed on them by activities other than cyber defense.

Initial explorations have identified the key functions, components and their interactions for a potential reference architecture of such an agent. However, it is beyond the current state of AI to support an agent that could operate intelligently in an environment as complex as the real battlefield. A number of challenges are yet to be overcome. The agents must be effective in an unstructured, unstable, rapidly changing, chaotic, adversarial environments; able to learn in real-time and under extreme time constraints, using only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive. At the same time, a growing body of research in the U.S. Government and academia demonstrates promising steps towards solving some of these challenges, and the industry is beginning to embrace approaches that may contribute to technologies of autonomous intelligent agents for the cyber defense of the Army networks. 

DISCLAIMERS

The views expressed in this paper are those of the author and not of his employer; they are not to be construed as an official Department of the Army position unless so designated by other authorized documents. Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

NOTES

Mohammed Noraden Alsaleh, Wei Jinpeng Wei, Ehab Al-Shaer, “Extractor–Automated Extraction of HoneyThings for Resilient Deception Planning based on Dynamic Malware Analysis,” presented at the ARO Workshop on HoneyThings: Autonomous and Resilient Cyber Deception, 2017.

M. T Azim, I. Neamtiu, and L. M. Marvel, Towards self-healing smartphone software via automated patching. *In Proceedings of the 29th ACM/IEEE international conference on Automated software engineering*, September 2014, 623-628.

R. J. Chang, R. E. Harang, and G. S. Payer, Extremely lightweight intrusion detection (ELIDe) (No. ARL-CR-0730). ARMY RESEARCH LAB ADELPHI MD COMPUTATIONAL AND INFORMATION SCIENCES DIRECTORATE, 2013.

Fan Fei, Tu Zhan, Yu Ruikun, Kim Taegyu, Zhang Xiangyu, Xu Dongyan, and Deng Xinyan Deng, “Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks.”, International Conference on Robotics and Automation, May 21-25, 2018, Brisbane, Australia.

S. L. Freedberg Jr., Missile Defense for Tanks: Raytheon Quick Kill vs. Israeli Trophy, *Breakingdefense.com*, March 9, 2016.

Gartner, “Magic Quadrant for Endpoint Protection Platforms,” January 2018, <https://www.gartner.com/doc/reprints?id=1-4PGZBYN&ct=180125&st=sb>.

B. K. Hall, Autonomous Weapons Systems Safety, *Joint Force Quarterly* 86, July 2017, <http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-86/Article/122391/autonomous-weapons-systems-safety/>, 86-93.

F. Y. Ken, and R. E. Harang, Machine learning in malware traffic classifications. *In Military Communications Conference (MILCOM)*, MILCOM 2017-2017 IEEE, 2017, October, 6-10.

A. Kott, A. Swami and P. McDaniel, Security outlook: six cyber game changers for the next 15 years. *Computer*, 2014, 47(12), 104-106.

A. Kott, L. Mancini, P. Théron, M. Drašar, E. Dushku, H. Günther, M. Kont, B. LeBlanc, A. Panico, M. Pihelgas, and K. Rzađca, Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense. *arXiv preprint arXiv:1803.10664*, 2018.

Alexander Kott, “Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments.” *arXiv preprint arXiv:1803.11256*, 2018.

A. Kott, C. Wang, and R. Erbacher, eds., *Cyber Defense and Situational Awareness*. New York: Springer, 2014.

A. Kott, D. Alberts, and C. Wang, Will Cybersecurity Dictate the Outcome of Future Wars? *Computer*, 48(12), 2015, 98-101.

A. Kott, R. Singh, W. McEneaney, and W. Milks, Hypothesis-driven information fusion in adversarial, deceptive environments. *Information Fusion*, 12(2), 2011, 131-144.

A. Kott and D. Alberts, How Do You Command an Army of Intelligent Things? *Computer* 12, 2017, 96-100.

A. Kott, A. Swami, and B. West, The Internet of Battle Things. *Computer* 49, no. 12, 2016, 70-75.

Alexander Kott and William M. McEneaney. *Adversarial reasoning: computational approaches to reading the opponent’s mind*. Chapman and Hall/CRC, 2006.

Vivienne Machi, “Army Rolling Ahead With Manned-Unmanned Convoys,” *National Defense*, April 4, 2018, <http://www.nationaldefensemagazine.org/articles/2018/4/4/army-rolling-ahead-with-manned-unmanned-convoys>.

I.Muttik, Good Viruses. Evaluating the Risks, Talk at DEFCON-2016 Conference, <https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-muttik.pdf>, 2016.

N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. Celik, and A. Swami, The limitations of deep learning in adversarial settings. *In Security and Privacy (EuroSecP)*, 2016 IEEE European Symposium, 372-387.

B. Piekarski, A. Mathis, W. Nothwang, D. Baran, C. Kroninger, B. Sadler, L. Matthies, V. Kumar, I. Chopra, S. Humbert, and K. Sarabandi, *Micro Autonomous Systems and Technology (MAST) 2016 Annual Report for Program Capstone. Technical Report ARL-SR-0377*. US Army Research Laboratory, Adelphi, MD, United States, 2017.

NOTES

R. Rasch, A. Kott and K. D. Forbus, AI on the battlefield: An experimental exploration. *In Proceedings of the Fourteenth Innovative Applications of Artificial Intelligence Conference on Artificial Intelligence*, Edmonton, Alberta, Canada, 2002.

S. Russell and P. Norvig, *Artificial intelligence: a modern approach*. 3rd ed. Upper Saddle River (NJ): Prentice Hall, 2009.

P. Scharre, *Robotics on the Battlefield Part II: The Coming Swarm*, Report, Center for a New American Security, Washington, DC, 2014.

M. R. Stytz, D. E. Lichtblau, and S. B. Banks, Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment. Report, Institute for Defense Analyses, Alexandria, VA, 2005.

P. Theron, A. Kott, M. Drasar, B. LeBlanc, K. Rzacca, M. Pihelgas, L. Mancini, and A. Panico, Towards an active, autonomous and intelligent cyber defense of military systems. *In Proceedings of the ICMCIS-2018 Conference*, Warsaw, Poland.

Don Woodard, "Deception and Decoy Autonomous Agent", in *Proceedings of the NATO IST-152. Workshop on Intelligent Autonomous Agents for Cyber Defence and Resilience*, Prague, Czech Republic, October 18-20, 2017, <http://ceur-ws.org/Vol-2057/>.

AI in Cyberspace: Beyond the Hype

Fernando Maymí
Scott Lathrop

Artificial intelligence (AI) is quickly becoming ubiquitous, particularly as part of solutions to defense problems in cyberspace. It seems like few companies want to risk marketing products that cannot be described using this term, perhaps for fear of losing ground to competitors who can. But what exactly is meant by AI? Is it all just marketing hype? The answer, of course, is far from simple. To move beyond the hype, we need to look at what AI is, what it is not and how the technology needs to mature to live up to its promise.

What it is

AI is a multidisciplinary field primarily associated with computer science, with influences from mathematics, cognitive psychology, philosophy, and linguistics (among others). The term was originally coined at a Dartmouth College workshop in 1956 and continues to be characterized by cycles of excitement, marvel, and disappointment as we come to grips with and gain a better understanding of both its promises and limitations. Depending on who you ask, AI's goals range from creating general intelligent systems to modeling human cognitive processes, to achieving superhuman performance on very specific tasks. An example of this is what we are beginning to see in image recognition systems through a machine learning technique called deep learning (more on that later). For this article, we are focused on defining AI in terms of how it can improve the functionality of a system so that certain tasks require decreased human involvement and intervention.



Fernando Maymí, Ph.D., CISSP, is Lead Scientist in the Cyber and Secure Autonomy Division of Soar Technology, Inc., an artificial intelligence research and development company where he leads multiple advanced research projects developing autonomous cyberspace agents for the Department of Defense. Dr. Maymi is a retired Army Officer with more than 25 years of service; he was the first Deputy Director of the Army Cyber Institute at West Point, an organization he helped grow and lead from its inception, and a former West Point faculty member. Dr. Maymí holds three patents and regularly consults on cybersecurity issues both in the U.S. and abroad. He is the author of numerous publications including the best-selling *CISSP All-in-One Exam Guide*.

From a historical perspective, what is considered AI today may not be considered “intelligent” or “cutting-edge” tomorrow. In the 1980s, a grammar checker seemed intelligent though such algorithms are now just part of word processing software. When web search started, people were amazed at search engines such as Google. Voice recognition is now integrated into our daily lives through technology such as Amazon’s Alexa™ and Apple’s Siri™; these AI technologies seemed “intelligent” when they first arrived on the scene but are now simply part of our lives. In the future, the same will be true for driverless cars, and other AI adopted technology.

At a high level, AI can be divided into two different approaches as shown in Figure 1 ^[1]: symbolic and non-symbolic; the key difference is in how each represents knowledge. Both approaches are concerned with how knowledge is organized, how inference proceeds to support decision-making, and how the system learns. For example, a spam filter may organize knowledge about an email message as a vector of words. The system learns as it is trained on whether messages are spam or benign. This training adjusts the system’s internal knowledge model. After training, each time a new email message arrives, the trained system infers whether the message is spam by comparing its features to the system’s underlying knowledge model.

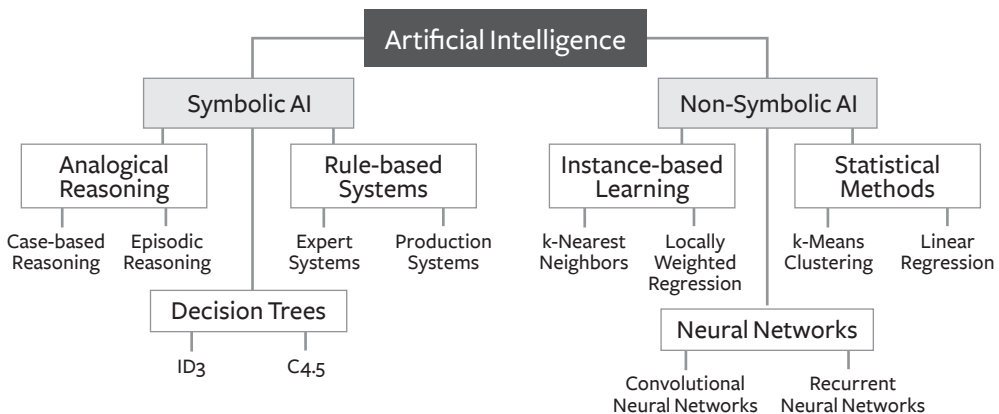


Figure 1: A partial taxonomy of artificial intelligence



Scott Lathrop, Ph.D., CISSP, is Soar Technology's Director of Cyber and Secure Autonomy. Before joining SoarTech, Dr. Lathrop served 26 years as an officer in the Army with his last military assignment as the Director of Research & Development at the United States Cyber Command where he led the delivery of multi-million-dollar full spectrum, technically assured, cyberspace capabilities as the Chief Technology Officer to Commander/Director USCYBERCOM/NSA. Prior to USCYBERCOM, Dr. Lathrop served as an Associate Professor in the Department of Electrical Engineering and Computer Science at the United States Military Academy, designing West Point's initial cybersecurity program, helping stand up the robotics program, and directing the Artificial Intelligence courses. Dr. Lathrop is a renowned author in the cognitive architecture community, publishing on mental imagery and applying cognitive architectures to robotics and cyber-entities.

Symbolic AI

In symbolic approaches to AI, system developers model real-world concepts, their relationships, and how they interact to solve a set of problems using a set of symbols (e.g., words or tokens). These AI approaches commonly use ontologies to organize knowledge and heuristic-based rules to support reasoning. Symbolic systems may also learn, such as learning a decision tree based on provided examples or through learning an appropriate decision based on previously recorded, similar events. Symbolic AI requires considerable *knowledge engineering* of both the problem and solution domains, which makes it fairly labor-intensive. However, it yields results that are inherently explainable to humans since they are derived from human knowledge models in the first place. Symbolic AI systems include the expert systems that became prolific in the 1980s. These relied on extensive interviewing of subject matter experts and time-consuming encoding of their expertise in a series of conditional structures. Unsurprisingly, these early systems were unable to adapt or learn absent human intervention, which is a problem when we consider the number of exceptions that apply to almost all processes.

The systems developed as part of the DARPA Cyber Grand Challenge are primarily symbolic AI systems. These automated reasoners can identify vulnerabilities in software services, develop a patch, and deploy the patch at machine speed. To create these systems, the teams encoded the knowledge associated with the types of vulnerabilities they might find (a form of an ontology), the procedures for finding the vulnerabilities (search and reasoning), and possible methods to remediate those vulnerabilities (decision-making). The systems learned in the sense that they were able to explore their environment (i.e. the network that they were a part of) and identify vulnerable services. However, that learning did not include finding new

vulnerabilities for which they were not previously encoded to identify. Furthermore, the systems did not learn how to identify new vulnerabilities by being trained on previous vulnerabilities through offline learning (i.e., learning from data before the system is deployed), which is common in the non-symbolic, statistical machine learning approaches discussed below. Nonetheless, these systems generated impressive results and will prove useful as we continue to investigate ways to make cyber defense more autonomous.

Modern symbolic systems are exemplified by cognitive architectures that emulate the way in which our human brains work. Systems like Carnegie Mellon University's Adaptive Control of Thought - Rational (ACT-R) and the University of Michigan's Soar (both open-source projects) are commonly used to build AI systems that can solve large sets of complex, real-world problems. Like their early symbolic predecessors, ACT-R and Soar require a fair amount of knowledge engineering in the form of building cognitive models to bootstrap them. Unlike early systems, however, these newer cognitive frameworks are capable of learning through interactions with their environments without human assistance and incorporate non-symbolic, machine learning approaches as part of their architectures. These "co-symbolic" (i.e. a hybrid symbolic/non-symbolic system) approaches appear to be where AI is heading as it takes advantage of the non-symbolic learning with the explainability of symbolic systems.

Non-symbolic AI

Another approach to AI departs from the use of symbolic representations of human knowledge and focuses instead on learning patterns in data for classifying objects, predicting future results, or clustering similar sets of data. Non-symbolic AI approaches are where many of the most recent advances have occurred, primarily in classification tasks such as image and voice recognition. In the current vernacular, these non-symbolic approaches are commonly called machine learning (ML) even though, as we just discussed, symbolic systems may also learn. As with symbolic approaches, non-symbolic ML systems also incorporate knowledge representations and reasoning. The knowledge representation is typically quantitative vectors (i.e., non-symbolic) with features from the dataset that describe the input (e.g., the pixels from an image, frequencies from an audio file, word vectors). Whereas symbolic AI requires considerable knowledge engineering, non-symbolic AI generally requires significant *data acquisition and data curating*, which can be labor-intensive even for domains where data is readily available. However, rather than having to program the knowledge as in a symbolic system, the non-symbolic ML system learns its knowledge, in the form of numeric parameters (i.e., weights), through offline ^[2] training with datasets with millions of examples. The most successful non-symbolic ML approaches today are *supervised learning*, where the datasets include a label or the "answer" for the correct classification. As training progresses, the ML model learns the correct parameters (i.e., weights) that minimize a cost function enabling the match of input patterns to an output classification or prediction. Reasoning then occurs when the trained ML model receives input from the operational environment and infers a classification.

Classification determines the class of a new sample based on what is known about previous samples. A common example of this is an algorithm called k-Nearest Neighbors (KNN), which is a supervised learning technique in which the nearest k neighbors influence the classification of the new point (e.g., if more than half of its k nearest neighbors are in one class, then the new point also belongs in that class). For cybersecurity, this is helpful when trying to determine whether a binary file is malware or detecting whether an email is spam.

Prediction compares previous data samples and determines what the next sample(s) should be. If you ever took a statistics class in college, you may recall a type of analysis called regression, in which you try to determine the line (or curve) that most closely approximates a sequence of data points. We use the same approach to prediction in ML by learning from previous observations to determine where the next data point(s) should appear, which is useful for network flow analysis.

In clustering, or *unsupervised learning*, on the other hand, we do not have a preconception of which classes (or even how many) exist; we determine where the samples naturally clump together. One of the most frequently-used clustering algorithms is k-Means clustering, in which new data points are added to one of the k clusters based on which one is closest to the new point^[3]. Clustering is useful for anomaly detection.

Finally, *reinforcement learning* tunes decision-making parameters towards choices that lead to positive outcomes in the environment. For example, one might have a security analyst provide feedback to an anomaly detector when it incorrectly classifies a benign alert as malicious (i.e., false positive). This feedback adjusts the internal model's weights so that the anomaly classification improves.

ML can be divided into two schools of thought. The first school tries to model the physiology of the brain and, specifically, the roles of neurons and synapses. This school gave rise to artificial neural networks, which break down complex problems into a multitude of tiny problems. For example, the problem of finding a face in a photograph is commonly broken down into problems such as deciding whether an eye, nose, and ear are in the frame and whether they are in the correct locations relative to each other. The “connection” between neurons is a simple mathematical function so that the output of the first neuron (e.g., there is an eye in the frame) is fed into the input of the next connected neuron by a multiplicative parameter that determines the weight of the connection. These parameters, or weights, are what are adjusted through algorithms such as backpropagation that enable the system to learn to match the input pattern to the desired output classification or prediction.

Neural networks are assembled into layers so that neurons in the same layer seldom pass data to each other and, instead, pass it to the next layer. The more layers you have, the more complex the problem you can classify or predict (e.g., the difference between classifying handwritten digits versus classifying dogs and cats in an image). A neural network with

many layers¹⁴) is considered capable of deep learning. A fairly deep neural network will require significantly more computing resources and training data than its “shallow” brethren. Therefore, depending on the problem at hand, deep learning may be an undesirable overkill.

The second school of thought in ML dispenses with any attempt to model physiology and focuses instead on mathematical algorithms that exploit anything from Euclidian distance to statistical regression to probabilistic (e.g., Bayesian) methods. Regardless of to which school it belongs, all ML is focused on specific features of the data (e.g., source IP address, interarrival rate). Given enough prior data, we can usually find good ways to classify, predict, or cluster new observations. The catch is that many, if not most, cybersecurity applications, require labeled (or at least partially labeled) data sets that represent the statistical distribution of the data in the operational environment. This means that if we want to train a supervised ML system to recognize malicious traffic, we need that traffic to be labeled as such and it must be representative of the number of malicious samples we would see in the real world. Acquiring these realistic and sufficiently large sets of labeled training data is often a significant challenge.

What it is not

AI has shortcomings that one must consider before employment. Neither symbolic nor non-symbolic AI approaches cope well with novel situations and require a human to re-engineer (symbolic) or retrain (non-symbolic) the algorithms. Symbolic, knowledge-engineered systems may contain underlying biases of the individual(s) who encode the system. Training data sets for non-symbolic approaches may contain biases that are not representative of the operational environment. These biases lead to either false positives, or worse, false negatives when the system is deployed. Such situations ultimately erode a user’s trust, especially if the user has no avenue to investigate how the underlying AI arrived at its decision. This problem can be exasperated with non-symbolic approaches as they are steeped in mathematical equations. The underlying reasoning that supports inferences is inherently uninterpretable. Users of these systems do not have a way to interact with the system, question it, and receive an explanation as to how it arrived at its decision.

There are also cybersecurity concerns related to the employment of AI. Non-symbolic, ML systems can be spoofed by introducing imperceptible variations into the input, thereby causing a cybersecurity product to change its classification of a malicious document from “bad” to “good.” Because both symbolic and non-symbolic AI systems are designed to make progress towards multiple goals, cyber-attackers could inject data into the environment that leads to goal conflicts, resulting in undesirable behaviors. For example, in swarm systems, modifying the perceived goal of a single agent could cause the entire multi-agent swarm to act unpredictably. To address these issues, AI systems will need to bring situational context to bear and use that context to determine whether the situation is in line with expectations. Outcomes that do not fit expectations would then be cued for further investigation and provide opportunities for additional learning.

Where we are

We need synthetic agents that can act as our teammates in cyberspace, particularly in Defensive Cyberspace Operations (DCO). The task is daunting because of the breadth of capabilities that such an agent would need. Below are some of the most important ones.

- ◆ **Sense.** Though we have many ML systems that can sense a variety of phenomena in cyberspace, these platforms are narrowly focused on specific applications. What we need is a generalized ability to ingest and integrate information from multiple sources for a variety of purposes. Ideally, humans and synthetic agents would use the same tools for sensing the environment so that sensors can be operated by either.
- ◆ **Think.** Autonomous agents make decisions based on what they sense in their environment combined with what they already know. At a minimum, the agents must respond appropriately to events for which they have an “approved solution” and investigate ambiguous situations when the situational context does not meet their expectations to understand and make adjustments. They should also experiment with novel solutions to new situations, learning what works and what doesn’t along the way.
- ◆ **Communicate.** If they are to be true teammates, our synthetic counterparts must know when and how to share information with their human counterparts. Their speed and capacity will preclude sharing everything in real time, but they must spontaneously reach out to their human supervisors when encountering specific situations and before embarking on risky exploratory behavior. The idea is to move the human to be *on* the loop instead of *in* it. Obviously, the agent must be able to respond to orders and questions from its human teammates and explain what it is doing and why in terms humans can understand.
- ◆ **Act.** It does us no good for agents to detect incidents and then not be able to respond autonomously. Clearly, we’d want to put bounds on risky responses, but faced with the eventuality of synthetic attackers, we can’t afford to wait on significantly slower human responses. This act capability is the counterpart of the sense capability discussed earlier. Similar to sensing, the agents should influence their environments using tools that they could exchange with their human teammates at any point in an operation.
- ◆ **Learn.** In many ways, this is the most mature of the five requirements. We have a variety of learning mechanisms for both symbolic and non-symbolic AI that allow autonomous agents to improve their performance and adapt to changing environmental conditions. Still, we have some work to do improving agents interactions with a variety of human and synthetic teammates. We also need them to learn the adversary’s behavior at a cognitive level rather than just recognizing their tools and left-behind indicators.

For the past two years, we have led research work on developing prototypes of offensive, defensive, and generic cyberspace agents that explore some of the building blocks required to provide these five capabilities. This family of synthetic teammates, called Cyber Cognitive (CyCog) agents is depicted in Figure 2. They all share a core system (CyCog) that they each refine with additional capabilities; this allows for time savings through software reuse.

The attacker version, CyCog-A, is intended for penetration testing and adversarial emulation during training events. CyCog-D is its defensive counterpart, which has only been used in support of training but already incorporates features that would allow it to effectively modify firewall and intrusion detection system (IDS) configurations in response to attacks. Finally, we are developing generic persona agents (CyCog-P) that behave as cyberspace denizens modeled after real users of a network under study.

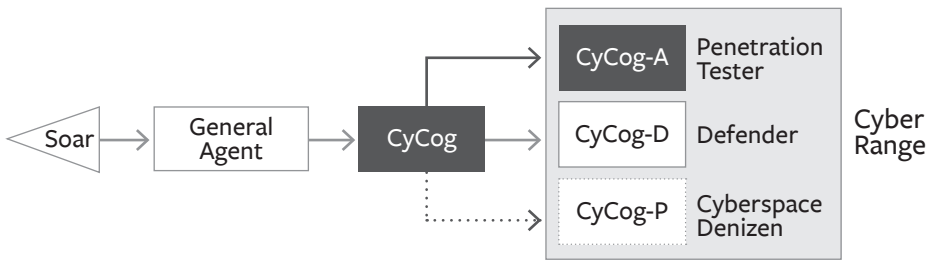


Figure 2: Genealogy of Cyber Cognitive (CyCog) agents

Because these agents are built on the Soar cognitive architecture, primarily a symbolic form of AI with some inherent non-symbolic features to support reinforcement learning and spatial reasoning, their cognitive models are inherently understandable by humans. This feature is illustrated in Figure 3, where we show an example goal tree (i.e., decision-making process) with a leaf node indicating an actual on-net action (i.e., sending a phishing email). This representation is easy to follow as the behavior model follows the cognitive processes of an attacker. Recall, however, that the bane of symbolic AI is this need for human-built models. Wouldn't it be possible to build AI systems that autonomously generate these?

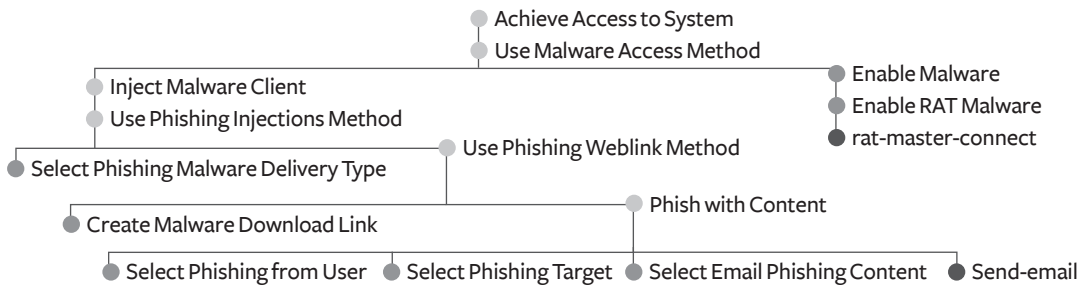


Figure 3: Partial CyCog-A goal tree showing a successful phishing attack

As an initial exploration of this possibility, we are in the early phases of a research project for the Office of Naval Research that seeks to develop ML modules that observe cyberspace activities, piece them together into procedures, and finds interesting (i.e., anomalous) ones. Codenamed *Twiner*, this system will allow us to reason over the three layers of cyberspace as defined by the U.S. DoD: persona, logical, and physical. By doing so, we believe we'll be able to detect behavioral patterns that would not be evident by looking at just one of these layers. This project will lay the groundwork for the autonomous identification of adversarial procedures and techniques, which, in turn, will allow us to automatically generate behavioral models and thus overcome one of the great limitations of symbolic systems.

The road ahead

Followed to its logical conclusion, *Twiner* and *CyCog* exemplify the symbiosis that results from leveraging both symbolic and non-symbolic approaches. Each plays to its own strengths while mitigating the limitations of the other. We already discussed how we could build non-symbolic AI systems that could observe cyberspace activities and build behavioral models for the symbolic AI agents. Conversely, these agents would be able to reason and act over a much broader set of observations, problems, and solutions than a non-symbolic AI system ever could.

A key takeaway from this paper is that to realize the full potential of AI, we must integrate its various forms in order to offset the limitations of each. No one approach will be sufficient because each approach is optimized for one specific set of problems at the expense of others. We can see this sort of integration in our own brains. According to Daniel Kahneman in his bestselling book *Thinking, Fast and Slow*, our brains leverage two systems: system 1 is fast, automatic and very task-specific (analogous to non-symbolic AI), and system 2 is slower, effortful and able to make complex decisions (analogous to symbolic AI). We all have cognitive mechanisms that allow us to switch from one to the other, and so should our synthetic teammates.

Good bedfellows

This paper has chronicled where we started, where we are, and where we should be going in the development of AI for cyberspace. Along the way, we have provided a fair amount of details about AI and ML. So, with all this in mind, how can you tell when someone is using these terms appropriately and when they are just hyping and overusing the terms? Below are three ideas you can try the next time someone wants to sell you on their version of AI.

Ask lots of questions. This may sound obvious, but many of us hesitate to ask questions when we think we know very little about a topic. We also tend to assume that if others speak authoritatively, then they must know what they're talking about. Even if you do not fully understand the responses (and you should keep drilling until you find something that makes sense), the manner in which others respond to your probing questions will tell you a lot

about their level of knowledge and how their solution works. Keep in mind that they usually cannot tell how much you know about AI, so they may get uncomfortable and be betrayed by their speech and body language. For better results, combine questions with the next suggestion: term familiarity.

Be familiar with key terms. Recall that, at their core, non-symbolic (a.k.a. ML) techniques are most commonly used for three purposes: *classification* (e.g., *k-Nearest Neighbors* or KNN), *clustering* (e.g., *k-Means*), and *prediction* (e.g., *regression*). They all work on *features* of the data they analyze (e.g., source IP address, interarrival rate), typically require large *data sets*, and always have a non-zero *false positive* error rate. Conversely, symbolic techniques require modeling of human knowledge that typically involves *cognitive modeling* and/or *task analysis*. As a starting point, you can make a list of all the italicized terms in the preceding text and learn a bit more about them. Even a summary understanding of them will go a long way in helping you tell when someone is trying to bamboozle you.

Call a friend. Most of us cultivate a diverse professional social network. Odds are that you know a couple of people who know enough about AI to help you separate the wheat from the chaff. (If you do not, this would be a perfect time to start making such friends.) Find them and ask for their opinion. Better yet, bring them along when you meet whoever will present to you their AI-powered solution. If the presenter lacks honesty or expertise, your friend should be able to tell right away even if you can't. Otherwise, it will be helpful to have someone who can help you translate the lingo, so you understand what is happening under the hood. 🛡️

NOTES

1. As with all taxonomy classifications, such as the one in Figure 1, variations exist. For example, a symbolic, rule-based system can have non-symbolic mechanisms (e.g. reinforcement learning) and a non-symbolic approach can use symbols such as a neural network that outputs a classification label such as 'cat', 'dog' from an ingested image of pixels.
2. *Offline* learning occurs in an environment separate from where the system is deployed. *Online* learning is when the system learns as it is operating in its intended environment.
3. Despite using the same letter for their namesake variable, KNN and k-Means are entirely different algorithms for different purposes and with different requirements. The details, however, are beyond the scope of this paper.
4. It is not clear how many layers in a neural network one has to have before it is considered a deep neural network. Ten layers or more is often considered the benchmark.

Culture in a Murky World: Hijab Trends in Jihadi Popular Culture

Elizabeth Oren

Although at times subtle, the female Muslim community influences and shapes the international security environment and constitutes a rough median of 49 percent over the estimated 1.6 billion global Muslim population. ^{[1], [2]} At the nexus of security and culture, themes like *hijab* trends highlight cultural shifts and social undercurrents impacting women that have powerful effects on the International Community. Across Eurasia, state-actors ban hijab-styles domestically to counter radicalization, while jihadi-extremists target women with hijab-themed content to bolster recruitment. Considering that women are susceptible to extremist recruitment, how can we expand the perspective on issues affecting Eurasian Muslim women by understanding the jihadi popular culture?

Hijab memes in Jihadi popular culture

Currently, hundreds of Russian and Turkish-speaking women have found themselves awaiting trial in Iraqi detainee camps due to their associations with designated terrorist groups, primarily Islamic State (IS) fighting in the Levant Region. ^{[3], [4]} Although the women awaiting trial number only around 1500, the sub-culture they cultivate has had an enormous impact on our world. While it may be tempting to label this a regional issue, the cultural and ethnic backgrounds of those detained in Iraq are quite diverse as evidenced by the French national who received a life sentence. ^[5] Despite the nationality marked on passports or government identification, many of the women define their identity based on ethnicity and ancestral culture. In this group, most of the detainees share the common languages of Russian and Turkish because they originate from the North Caucasus region, Central Asia, and Turkey.



Elizabeth Oren is the Chief of Cyber Analytics for JACOBS Mission Operations Group supporting customers at USCENTCOM and USSOCOM. Ms. Oren's primary role is running the Cultural Analytics Research Laboratory. She was previously an analyst at USSOCOM, a fellow at the NATO School in Germany, and a counterterrorism researcher at the NATO Center of Excellence—Defense Against Terrorism (COE DAT) in Turkey. A grant from the University of Texas at Arlington allowed Ms. Oren to study Turkish and Machine Translation engines for agglutinative languages.

She holds a BA in History from Texas A&M University, and two BA's in Critical Area Studies for Russian and French from the University of Texas at Arlington. Ms. Oren has Foreign Language Studies and Translation Certifications in Russian, French, Turkish, and German.

Although some women have joined groups like IS because they were following husbands, boyfriends or other family members, some pledged loyalty solely based on ideology. Many people join jihadi aligned groups with the hope of a new beginning and a saved afterlife. Inherently, the community of jihadi-supporters forms a unique popular culture or pop-culture. Jihadi pop-culture has its own rules which change depending on the group and the cultures surrounding it.

For IS and some AQ-aligned groups, public gender mixing is taboo without a familial connection. Since communication is segregated, contact between women and men occurs indirectly. Just like mainstream social media, the meme is popular among extremist supporters. The power of the meme lies in the combination of emotive images and sharp phrases making it simple yet effective. As such, the meme is one of the more prevalent content forms in extremist forums that target Muslim women.

In the mainstream Muslim world, hijab is considered an Islamic duty and is not an extremist symbol in and of itself. Hijab manifests in many forms like the Chador, Khimar, Niqab, Burka or Al-Amira,^[6] and contemporary hijab fashion integrates styles from European haute-couture to Urban streetwear.^[7] There is a belief held by some Muslims that hijab can determine a woman's place in the afterlife because it protects her honor, family, and marriage. Since hijab is a valued standard and normal aspect of daily life in many Muslim societies, jihadi groups create content using hijab themes to attract women. The associated captions on memes are similar to *Meme 1* translating from Turkish to English as: "I am not



Meme 1. Turkish Language, 2018.

searching the good life; I am searching the good afterlife”.

Extremist content urges Muslim women to cover themselves, and the Qur’an and the Hadith are used as the justification. Hijab memes created by IS supporters depict women in black Niqab with the eyes veiled or in Burqa which completely covers the face. Since the eyes are considered the windows to the soul, which can flirt and entice, guidance follows that either the eyes should be veiled or mostly covered. Exceptions may be made in combat situations. One of the more controversial aspects of hijab in jihadi circles is whether the face, including the eyes, should be covered. While most agree to cover the face, AQ-aligned groups hold a less strict rule on covering the eyes, as the crowned female Muslim cartoon in Niqab in *Meme 2*, shows verse one and two from Al-Muddaththir, Surah 74, “O you who are cloaked!! Arise and warn!” [8], [9]



Meme 2. Turkish Language, 2018.



Meme 3. Russian Language, 2015.

In jihadi content, hijab should not reveal the shape of the body, and must be in the tradition of black to prevent jealousy from female and male onlookers. Hijab obliges women to seek approval from God, not man, and discourages false worshiping of material goods like make-up and unnatural beauty. *Meme 3* translates from Russian as, “We don’t need compliments from boyfriends or recommendations from magazines to know we are pretty. We know that we are beautiful, we know that we are queens...”

There are several details involved in wearing hijab in accordance with jihadi codes, and women seek compliance according to the extremist groups’ recognized imams. Thick fabric for hijab is imperative because transparent cloth reveals the body. The hands

should be covered by gloves as should the feet by closed-toe shoes and socks. Eye make-up is permitted, however, limited to black eyeliner in the tradition of the Sunnah. Although not encouraged, hair coloring is permitted if it resembles one’s original hue except black hair dye shouldn’t be too dark. A woman’s hair should be long without resembling a man’s cut. There are constraints on waxing facial hair and nail polish. Notably, plucking eyebrows and applying lipstick is taboo as *Meme 4* streaks through penciled eyebrows and pink tinted lips, noting “this kind of thing does not exist in Islam.”



Meme 4. Russian Language, 2015.

In the jihadist view, women who choose not to wear hijab as prescribed go against God’s Law, and the content attempts to scare and shame women as illustrated in *Meme 5*. A modernly clad woman with uncovered hair wearing a daisy-duke jean skirt and pink tank top descends via escalator to the fires of Hell. Meanwhile, the woman in a loose-fitting black hijab ascends to the bright light of Heaven. The Russian Cyrillic warns, “Dressed and at the same time naked, swaying while walking, and these tempting [actions] men and women will not go to Heaven and will not even breathe Heaven’s fragrance.” This references Hadith 1633 from the Book of the Prohibited Actions, but it has been abbreviated heavily. ^[10], ^[11] The paraphrasing of the Qur’an and Hadith is common with extremist propaganda, ^[12] and the consequence is reshaping ideology by novice followers on social media. When quotes from religious texts are without context or translated liberally, it contributes to misinterpretations that are splintering mainstream Muslim society. ^[13]



Meme 5. Russian Language, 2014.

Some Muslim women believe that one cannot truly abide by Islam while living in a country that does not enforce standards set by the Qu’ran and Sunnah. Also, appropriate clothing can be particularly challenging for Muslim women living in secular countries, and the mixed-gender social structures can cause stress. Groups like IS promote that women have the freedom to be proper Muslims within their community because ‘true’ hijab is mandatory and enforced. More so than other extremist groups, IS advertises a relaxed environment for women by establishing all-female shopping centers, city buses, and universities. By making an environment that appears conducive to these beliefs, extremist groups present women the opportunity to follow Islam easily.

Many hijab-inspired memes circulated on Russian and Turkish social media are not stamped with the moniker of an extremist organization. The content appears user-generated, which most of it likely is, and the popularity of the content is innately linked to this organic style of messaging. Since the content seems purely religious, the memes are shared pervasively across social media. The cultural themes in the content speak to truths about hijab, modest appearance, and women in society that resonate with social undercurrents impacting many Muslim communities.

Hijab memes in Muslim popular culture

For many Muslim women, hijab is a personal subject influenced by family tradition. As such, hijab styles and norms in one country may be completely different than in another, and the same goes for families in the same country. For example, Niqab is the norm in Saudi Ara-

bia, but a headscarf and loose-fitting clothing are norms in Chechnya. In Turkey, hijab may be the norm for one family while the neighbor across the street does not conform to any style of hijab. Since neither Niqab nor Burqa are recent norms in Russian and Turkish-speaking communities, the social push online for this change indicates a cultural shift in these societies.

The principal argument against modern hijab styles in Russian and Turkish language content is the perceived negative influence of Western modernity on Muslim women. In Russian-speaking Muslim societies, many women wear headscarves and a combination of long or knee-length skirts, and full or three-quarter length tops. Generally, the style is fitted and colorful, and the headscarf does not always cover all the hair or the face. Women also wear makeup, color their hair, and wear high-heels.

In a rebuke against this trend, some users try to shame Muslim women through content like *Meme 6*, “Recognize! You are a modest Muslim woman, in agreement for the sake and satisfaction of Allah / or a show-off, pleasing Satan, and who doesn’t know the point of the veil.” In *Meme 7*, we see a woman wearing a fitted, full-length blue dress, ornate necklace, and a fitted headscarf. This is an example of current hijab fashion popular in Russia, in which the body and hair are covered, and the clothing is fitted and colorful. The creator of *Meme 7* contrasts an image of a woman dressed in Niqab; the quote reads, “Women who say, ‘tons of men chase after me’, Remember—the lowest price always attracts the most buyers.”



Meme 7. Russian Language, 2015.

defined by full length or three-quarter length overcoats, long skirts, loose-fitting tops, and a wrapped yet loose decorative headscarf. In *Meme 8*, we see two women modeling Turkish hijab fashion contrasted with a woman in black Burqa. The quote reads, “In your opinion, who is wearing hijab???” The point here is that Turkish hijab fashion does not represent ‘true’ hijab.

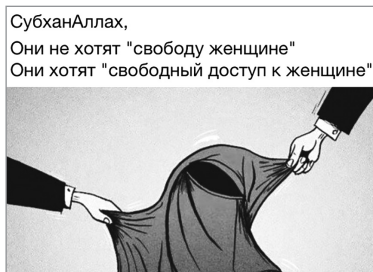


Meme 6. Russian Language, 2014.

Turkish fashion is popular among Muslim women throughout Eurasia, and there are many Russian-speaking Muslims in Turkey. Turkish hijab fashion can be very colorful and



Meme 8. Russian Language, 2014.



Meme 9. Russian Language, 2015.

never take it off. Remember that the undressed woman will fight off men like flies.”

Many Muslims believe hijab is an obligation to God, liberation from unattainable ideals of beauty, and protection from men and consumerism. Accepted truths about hijab and women in modern society appear in extremist content, and it makes the message reach a broader audience. To a lesser yet important extent, this recruitment dynamic reaches women from non-Muslim and un-religious backgrounds, [14]

because they are affected by the real issues layered within the content. At times Western societies misinterpret societal and cultural realities that affect Muslim women living abroad. This hinders our ability to appreciate the complexities behind extremist recruitment.

Hijab norms and cultural shifts

In the context of international security, there is a fine line to tread interpreting the nuances of hijab and the correlation to violent extremism. How do we tell the difference between jihadi supporters and the simply religious? This is a struggle many families, communities, and state actors grapple with throughout the world. Before dangerous assumptions unravel liberty, it is imperative to recognize cultural and religious norms before identifying alarming changes in society.



Image 1. Daghestani Traditional headdress, Kamil Chutuev, 2009.

For some Muslim women, hijab is liberation from modern expectations of female appearance. In their view, fashion distorts beauty and objectifies women for money and the pursuits of men. *Meme 9* exclaims, “SubhannaAllah, They do not want ‘Free Women;’ They want ‘Free access to women.’” *Meme 10* illustrates an unwrapped lollipop to express the protection that hijab offers women, “Little sister, keep your hijab and

never take it off. Remember that the undressed woman will fight off men like flies.”



Meme 10. Russian Language, 2015.

At times Western societies misinterpret societal and cultural realities that affect Muslim women living abroad. This hinders our ability to appreciate the complexities behind extremist recruitment.

For women from the Gulf States like Saudi Arabia, Niqab, Abaya, and face-veils are a norm and do not necessarily correlate to extremism. There are hijab traditions endemic to Turkic and Caucasian women dating back to Ottoman times, which resemble Niqab and face-veils. [15], [16] In the Caucasus Region, some women wore cloaks with ornate adornments as seen by the Daghestani girl in *Image 1*. [17] While other women covered with Abaya styles as depicted in *Meme 11*; [18] the text declares, “Our ancestors didn’t know what ‘Hijab’ was. They knew what shame and Faith were.”

Conservative hijab is not a foreign concept for many Muslims but depending on the style some leaders of Muslim nations fear its revival. The Chechen Republic uses an elimination strategy against Wahhabism, which is associated negatively in the Caucasus region with all-black hijab and face-veils like Niqab. The fear is that a foreign, radical form of Islam will engulf the entire society and encourage the youth to join extremist groups. However, hijab is enforced socially in Chechnya, but it is limited to styles personifying Chechen heritage. ^[19] There are reports of Chechen men firing paintballs at younger women who are not fully covered, and some women find marriage without full-hijab difficult. ^[20], ^[21] The concept is to foster Islam and piety among the population while maintaining cultural identity and fighting an ongoing twenty-year insurgency.



Meme 11. North Caucasian Women, 1900s.

For Chechnya at least, the governmental enforcement of hijab represents a shift when compared to Soviet times and post-Soviet 1990s, when many women did not wear headscarves and sported short sleeve shirts and shorter skirts as seen more commonly today in Dagestan. ^[22] Whether living in the Russian Federation or as refugees abroad, Muslim women from the North Caucasus are a particularly vulnerable population because their liberty is tied heavily to social perceptions of modesty, honor, and piety, which is only intensified by governmental influences that deviate from secularism. The extremist recruitment of women and the popularity of jihadi content among this demographic is not surprising given the circumstances.

Turkish women are known in the Caucasus Region and Central Asia for having many liberties such as the freedom to work, study, dress, drink, smoke, and socialize. This was further influenced after the founding of the Turkish Republic in 1924 by Kemal Ataturk, who spearheaded secular reforms that encouraged women to wear Western fashions and restricted the Ottoman-era veil in public institutions. ^[23] However, in 2013 the Turkish Republic removed the hijab-ban under the pretense of religious freedom, thus allowing women to wear the veil at work and university. ^[24] For some women, this means the freedom to express Islamic duties. Yet, some women in Turkey feel social pressure to wear hijab since the ban reversal, ^[25] and face harassment stereotyped as immodest for dressing in the secular tradition of their mothers. In the case of Turkey, lifting the ban gave religious freedom to those who felt marginalized for years, but it also forecasts the extremist environment in Turkey for the years to come.



Image 2. Traditional Tajik hijab, 2018.

Contrary to Chechnya and Turkey’s approach, other nation-states are taking counter-radicalization strategies that ban certain types of hijab. In Tajikistan, hijab trends like black Burqa deviate from traditional Tajik culture, as depicted in *Image 2*,^[26] and authorities are reportedly banning the sale of Burqa in markets and barring it from public spaces.^{[27], [28]} The State Islamic University in Indonesia, home to the world’s largest Muslim population, banned Burqa in 2018 due to the concern of extremist propagation.^[29] Similarly, in European countries like France, Denmark, and the Netherlands, Burqa is viewed as dangerously close to terrorism, which resulted in these Western countries banning face-covering hijab

styles.^{[30], [31], [32]} Hijab can represent a cultural shift too far from the norm for certain states that the only option seems to be banning the veil, which brings into question the effectiveness of limiting religious liberties to counter radicalism.

While it may seem decisive to ban face-veils and hijab to curb extremism, it can exasperate marginalized populations. Around 2013, the Russian Federation banned hijab in schools notably affecting a large Muslim population in Stavropol Krai.^[33] Since the ban inhibits Muslim families from raising their children according to religious beliefs, it is viewed as just another aspect added to the difficult reality for life as a Muslim in Russia. Collectively, nationals who are descendant from ethnicities native to the Caucasus Region and Central Asia represent a large portion of IS and AQ-aligned group supporters.^[34] Frequently, religious oppression such as banning hijab, regardless of the style, is cited as a reason for supporting a jihadi cause.

As with most trends in international security, nothing is clear-cut, and the social undercurrents affecting the female Muslim community are no exception. Ultimately, nations will have to find the balance between liberty and security to avoid creating oppressive environments that foster extremism. This is particularly challenging with immigration rising from war-torn countries, foreign fighters attempting to reenter society, and global communications enabling the proliferation of extremists’ ideology.

Regardless of the number of supporters, jihadi-groups inflict a disproportionate amount of damage on nations relative to their small sizes and seemingly innocuous pop-cultures. As of 2017, the US Government totaled the cost of Operation Inherent Resolve at 14.3 billion dollars.^[35] Cultural Analytics only serves to enhance our efforts by injecting a different perspective on the people and communities influencing operations. The better our awareness of complex cultural nuances, the more apt our approach will be at recognizing its applicability and navigating the ambiguity of the international security environment.♥

NOTES

1. Drew Desilver and David Masci, January 31, 2017. World's Muslim population more widespread than you might think. Pew Research Center. <http://www.pewresearch.org/fact-tank/2017/01/31/worlds-muslim-population-more-widespread-than-you-might-think/>.
2. The World Bank, 2017, Population, female (% of total), The World Bank Data, <https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS>.
3. Fehim Tastekin, March 8, 2018, Death Sentences cool warming Iraq-Turkey Ties. Al-Monitor, Turkey Pulse, <https://www.al-monitor.com/pulse/originals/2018/03/turkey-iraq-sentences-turkish-women-to-death.html>.
4. Iraq court sentences French women to life for IS membership: AFP, June 3, 2018, France 24, <http://www.france24.com/en/20180603-iraq-court-sentences-french-woman-life-membership-afp>.
5. Iraq: 19 Russian women handed life sentence for joining ISIL, April 29, 2018, Al Jazeera, News/ISIS, <http://www.france24.com/en/20180603-iraq-court-sentences-french-woman-life-membership-afp>.
6. What's the difference between a hijab, Niqab and burka? June 18, 2015, BBC, Newsround, <https://www.bbc.co.uk/newsround/24118241>.
7. Janie Har, San Francisco museum shows off modern Muslim women's fashion, September 21, 2018, Fox News, Islam, Associated Press, <http://www.foxnews.com/us/2018/09/21/san-francisco-museum-shows-off-modern-muslim-womens-fashion.html>.
8. Al-Muddaththir 1 and 2, Surah 74 The One Enveloped, Islam in Quran, www.islaminquran.com/en-US/surah-74/al-muddathtur/ayat-2/quran_ayats.aspx.
9. Towards Understanding the Quran, Surah Al-Muddaththir 74:1-7, Islamic Studies. www.islamicstudies.info/tafheem.php?sura=74&verse=1&to=7.
10. The Book of Prohibited Actions, Hadith 123, SUNNAH, www.sunnah.com/riyadussaliheen/18/123.
11. Riyad-as-Saliheen, [Muslim], Riyad Us Saliheen, Islamic Studies, www.Islamicstudies.info/hadith/riyad-us-saliheen/riyad.php?hadith=1631&to=1633.
12. <https://www.vox.com/2015/11/18/9755478/isis-islam>.
13. <https://en.qantara.de/content/social-media-against-islamic-extremism-an-invisible-battle>.
14. Paul Sperry, Meet the American women who are flocking to join ISIS, May 13, 2017, New York Post, Opinion, <https://nypost.com/2017/05/13/meet-the-western-women-who-are-flocking-to-join-isis/>.
15. Kamil Chutuev, Dagestan over the decades, September 9, 2013, RFERL, Photo Galleries, <https://www.rferl.org/a/photo-to-exhibition-culture-dagestan/25095654.html>.
16. Dr. Sumiyo Okumura, Women's Garments, Turkish Cultural Foundation, <http://www.turkishculture.org/textile-arts/clothing/womens-garments-1065.htm>.
17. Kamil Chutuev, Dagestan over the decades, September 9, 2013, RFERL, Photo Galleries, <https://www.rferl.org/a/photo-to-exhibition-culture-dagestan/25095654.html>.
18. Elizabeth Oren, Hijab Trends of the North Caucuses and Central Asia, (unpublished). 2015, NATO SCHOOL, Research.
19. Russia: Chechnya Enforcing Islamic Dress code, March 10, 2011, Human Rights Watch, <https://www.hrw.org/news/2011/03/10/russia-chechnya-enforcing-islamic-dress-code>.
20. <https://www.rferl.org/a/chechnya-islam-hijab-kidnapping/24940634.html>.
21. The Lives of Chechen Girls. March 27, 2013, RadioFreeEurope RadioLiberty, Photo Galleries, Reference article about paintball, <https://www.bbc.com/news/world-europe-12705300>.
22. Victoria Gurevich, The inequality of women keeps the North Caucasus vulnerable, June 12, 2017. ODR, Russia and Beyond, <https://www.opendemocracy.net/od-russia/victoria-gurevich/inequality-of-women-keeps-north-caucasus-vulnerable>.
23. Burak Sansal, Ataturk's Reforms, 2018, All About Turkey, History, <http://www.allaboutturkey.com/reform.htm#laik>.
24. Jeremy Bender, What 10 Turkish Women Really Think About the Headscarf. November 7, 2013, BuzzFeed. https://www.buzzfeed.com/jeremybender/women-share-what-the-headscarf-means-to-them?utm_term=.rdPP8pxJx#.xION-mEq3q.

NOTES

25. Fariba Nawa, Turkey's fraught history with headscarves, December 20, 2016, PRI, Religion, <https://www.pri.org/stories/2016-12-20/turkeys-fraught-history-headscarves>.
26. Pinterest. Tajik Dresses, <https://www.pinterest.com/bykhusen/%D1%82%D0%B0%D0%B4%D0%B6%D0%B8%D0%BA%D1%81%D0%BA%D0%B8%D0%B9-%D0%BA%D0%BE%D1%81%D1%82%D1%8E%D0%BC/>.
27. Tajikistan shaves 13,000 beards in 'radicalism' battle, January 21, 2016, Aljazeera, Asia News, <https://www.aljazeera.com/news/2016/01/tajikistan-shaves-13000-men-beards-radicalism-160120133352747.html>.
28. Harriet Agerholm, Tajikistan passes law 'to stop Muslim women wearing hijabs', September 1, 2017, Independent, News World Asia, <https://www.independent.co.uk/news/world/asia/tajikistan-muslim-hijabs-stop-women-law-head-scarfs-central-asia-islam-a7923886.html>.
29. World News, Indonesian Islamic university bans burqas on campus, March 7, 2018, Reuters, World News. <https://in.reuters.com/article/indonesia-religion-burqa/indonesian-islamic-university-bans-burqas-on-campus-idINKCNIGJ198>.
30. Denmark passes ban on niqabs and burkas. May 31, 2018, BBC, Europe, <http://www.bbc.com/news/world-europe-44319921>.
31. Madeleine Ngo, The Netherlands just passed a law banning face veils in public buildings, June 29, 2018, Vox, <https://www.vox.com/world/2018/6/26/17507086/muslim-women-dutch-netherlands-face-veils>.
32. Jake Cigainero, Five years into ban, burqa divide widens in France, October 4, 2016, DW, Europe. <https://www.dw.com/en/five-years-into-ban-burqa-divide-widens-in-france/a-19177275>.
33. Ellen Barry, Local Russian Hijab Ban Puts Muslims in a Squeeze, March 19, 2013, New York Times, Europe, <https://www.nytimes.com/2013/03/19/world/europe/russian-regions-hijab-ban-puts-squeeze-on-muslims.html>.
34. Ellen Barry, Local Russian Hijab Ban Puts Muslims in a Squeeze, March 19, 2013, New York Times, Europe, <https://www.nytimes.com/2013/03/19/world/europe/russian-regions-hijab-ban-puts-squeeze-on-muslims.html>.
35. Operation Inherent Resolve, Targeted Operations to Defeat ISIS, 2017 U.S. Department of Defense, Special Reports, <https://www.defense.gov/OIR/>.

Offensive Digital Countermeasures: Exploring the Implications for Governments

Rock Stevens

Jeffrey Biller

ABSTRACT

The theft of intellectual property and classified data within the cyber domain poses a threat to the global economy and national security. In this paper, we discuss the concept of digital offensive countermeasures that the United States can use to defend its sensitive data and intellectual property, even after stolen data leaves U.S. Government networks. We analyze the plethora of legal and ethical issues involving the various degrees of invasiveness posed by such defenses against both foreign and domestic targets. The lack of established norms surrounding digital offensive countermeasures presents a unique duality in which such defenses may present a viable cyber deterrent for the United States but may also spark our next conflict.

INTRODUCTION

Intellectual property (IP) and sensitive data theft in the cyber domain poses a threat to the global economy and national security. For example, the \$406.5 billion U.S. Department of Defense (DoD) F-35 Joint Strike Fighter program was the victim of multiple data breaches; moreover, the Chinese incorporated strikingly similar technology within their Shenyang J-31 stealth fighter which suggests that the United States (US) paid for the research and development for another country. ^[2]

The interconnectedness of businesses, governments, and the Internet makes it more appealing and viable for rival entities to reap immense technological boosts through IP theft. ^[3] Thus, corporations and governments must expand defensive efforts to make IP theft more difficult and costlier for attackers. Cybersecurity offensive countermeasures (OCMs) provide ways for achieving these goals. OCMs, also known as active defense strat-

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



Major Rock Stevens is an Army Cyber Officer and is a lifelong student of information technology, earning his first certification as a network administrator at the age of 15. He served as a Madison Policy Forum Military-Business Cybersecurity Fellow in 2015 and is pursuing a Ph.D. in Computer Science from the University of Maryland

egies, employ methods for achieving attack attribution, tracking intrusions back to their true source, and detecting attackers within networks.

Various OCMs are currently in use within the cybersecurity community, and they differentiate themselves along a spectrum of invasiveness. Honeypots represent the most benign end of the spectrum, in presenting attackers with a fake environment, permitting defenders to observe attackers' tactics and techniques, and allowing defenders to create defensive signatures that can block future intrusion attempts. On the opposite end of the spectrum, we re-introduce the controversial concept of allowing adversaries to steal tampered IP that, when utilized, will result in physical destruction. In this paper, we discuss and explore the legal, ethical, and policy issues in a nation that protects its sensitive data with various OCMs.

1. RELATED WORK

This section outlines state-of-the-art defensive measures, provides a survey of threat modeling techniques, and introduces various offensive countermeasures that allow defenders to protect sensitive data and detect intrusions. These measures serve to increase the difficulty for successful cyber intrusions. As a general disclaimer, no single method can be effective against all threats, and practitioners should intertwine defensive measures when possible to reap synergistic effects.

1.1 State-of-the-art defenses

State-of-the-art defensive measures represent an evolution of defensive techniques within a cyber arms race: malicious actors exploit systems, defenders observe offensive methodologies through forensic analysis of attacks, defenders learn how to prevent such attacks from happening again, and attackers develop innovative ways to bypass defenses. We provide a cursory survey of current-generation solutions that



Lieutenant Colonel Jeffrey Biller is an Air Force Judge Advocate and Military Professor at the United States Naval War College in the Stockton Center for the Study of International Law, where he acts as the Associate Director for the Law of Air, Space, and Cyber Operations. The Stockton Center is the college's research institute for the study of international law and military operations. Stockton Center faculty teach in the core curriculum and electives at the Naval War College, as well as in advanced international law courses around the world.

disrupt attackers' methodologies, mitigate the effectiveness of their tools, and provide defenders with an improved security posture. The common theme throughout these defenses is that they all fail to assist defenders once an adversary has already attained access to intellectual property. Network administrators have implemented technologies commonly referred to as zero-client networks, where desktop workstations are replaced by virtualized systems to eliminate adversarial persistence but fail to protect stolen data. ^[4] Zero-clients share a common secure baseline and exist only on demand; when a user logs in, a new version of the workstation is sent over the network. When the user logs out, the workstation is purged. This ephemeral characteristic requires attackers to continually re-infect targeted systems after each new session and prevents malicious actors from reliably using these systems within a botnet. If the secure baseline is frequently patched and assessed for vulnerabilities, zero-client networks can reduce the likelihood of external intrusions. This technology usually relies on network-wide databases for maintaining persistent information. These databases are not ephemeral nor is the data it stores; therefore, if an attacker can successfully exfiltrate sensitive data on these servers through an infected zero-client to an external destination, the zero-client technology is useless in protecting the stolen data. Thus, researchers have developed new technologies that aim to improve data access controls.

Zero trust networks (ZTN) represent an amalgamation of numerous permission-based security methods that can reduce external and internal threats from accessing sensitive data that zero-clients cannot protect. ^[5] The basic concept behind ZTNs is that everything starts from an untrusted baseline and trust is established through a combination of methods, giving system administrators fine granularity control

over how devices and users access data. Using an up-to-date device inventory, ZTNs can deny or reduce access to resources if the requesting device is not using updated patches. ZTNs can restrict access based on time of the day or by where a user is logged in from. By layering permissions, ZTNs can prevent attacks from compromised administrator accounts, the most trusted accounts within a domain. Clearly, these security methods increase the difficulty for an attacker to access IP, but ZTNs cannot assist defenders if IP is exfiltrated to an external system. ZTNs can establish a chain of custody for accessed data within an environment through high levels of logging.

The Open Web Application Security Project (OWASP) maintains a series of best practices that guide network defenders toward implementing secure systems.^[10] Such guidelines provide an effective service towards building a more secure community and lends itself as input for various offensive countermeasures that we outline in the following section.

1.1 Offensive countermeasures

Offensive countermeasures and active defense strategies provide an interactive means for detecting and mitigating attacks. Honeypots are arguably the most benign OCM and present attackers with a fake virtualized environment. While attackers are attempting to exploit vulnerabilities and steal data, honeypots permit defenders to observe adversarial tactics and techniques and allows the creation of defensive signatures that can block future intrusion attempts.^[16] Honeypots serve as an immediate means for alerting defenders to intrusions because there is no legitimate use for honeypots only malicious actors will try to access them.

The concept of honeypots gave way to several innovations. Honeyports are fake open ports that detect network scanning and enumeration attempts by unauthorized personnel.^[17] Honeywords consist of fake passwords or password hashes that administrators seed within databases; if someone attempts to login using one of these honeywords, it triggers an alarm to defenders that the malicious actors have compromised the database and are attempting an intrusion.¹⁸ All of the methodologies of the honeypot family provide defenders with immediate notice and allow them to mitigate future incidents.

Web bugs are the first OCM we discuss that provides defenders with attribution for IP theft. Web bugs are beacons embedded within documents that alert a central server anytime those documents are accessed, allowing the central server to log the source location and time of access. If the malicious actors are not using a virtual private network or TOR,²⁰ the central server logs their true location and defenders can begin to coordinate with law enforcement agencies for a formal investigation. Web bugs can be easily defeated if the malicious actor follows strict operational security and disables JavaScript within documents and uses location obfuscators at all times. Therefore, researchers developed new OCMs that would thwart attackers from discovering sensitive data.

Zip bombs are an OCM further along the invasive spectrum and are specifically designed

to conduct denial of service attacks on its victims and their storage resources.^[22] Zip bombs are crafted zip file archives that typically expand recursively and exponentially when an application unpacks it, or anti-virus application inspects it. The most famous zip bomb, 42.zip, is 42 kilobytes compressed and expands to 4.3 gigabytes;^[23] newer adaptations unpack infinitely until the victim crashes or the unpacking process is terminated. Coupling zip bombs with honeypots wastes the time of malicious actors while providing defenders with invaluable intrusion alerts.

These examples of OCMs present defenders with new methods for determining attack attribution and protecting intellectual property. When coupled with threat modeling techniques and other defensive strategies, defenders develop layers of security that increase the difficulty and cost of attacks for malicious actors. Nevertheless, these efforts may prove insufficient in the modern security environment and may require more overtly offensive methods. In the next section, we explore adaptations to traditional OCMs from this section that could lead to physical damage or destruction in the real world.

2. OFFENSIVE COUNTERMEASURES FOR NATION-STATES

In this section, we discuss various OCMs along a spectrum of invasiveness and discuss the possible legal implications of their use by state actors. The legal and policy concerns are driven both by the type of OCM to be employed and the context of their use. Therefore, we analyze each type of OCM first in their potential use against foreign targets, both within and outside of armed conflicts, and second, when the OCM has a domestic target. This article assumes that the state agency utilizing the honeypot has the appropriate foreign-intelligence, counter-intelligence, military, or law enforcement authority to conduct the operation utilizing the OCM.

We note at the outset that the application of law to the cyber domain is less than fully developed.^[25] International law often adapts slowly to new technology, as states create international obligations over time through a combination of formal agreements and customary law.^[26] There exist few formal international agreements related to cyber and customary law requires states to make formal pronouncements on their understanding of legal obligations.^[27] To date, states have been reticent to make such pronouncements on the application of international law to cyberspace, or even agree to basic international norms.

Several legal scholars have taken up the challenge and provided their interpretations of the application of existing law to cyberspace. The most in-depth and widely-cited of these efforts is the Tallinn Manual project, recently updated and expanded as the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. This manual primarily represents the opinion of nineteen international law experts, referred to in the manual as the International Group of Experts (IGE). Although this paper frequently references the Tallinn Manual 2.0 as an indication of scholarly opinion, we reiterate that only states can create international legal obligations.

2.1 Beaconsing implants

The most uncontroversial OCM involves implanting sensitive documents with a “beacon.” This type of OCM is already in general use as a counter-intelligence technique.^[28] These types of beacons alert the owner anytime an unauthorized user accesses a protected piece of intellectual property or sensitive document from an unauthorized location. Beacons vary in implementation but consist of an embedded application or script that sends information to a centrally-controlled server. This server, in turn, logs metadata associated with the access request, such as the internet address of the host computer, its operating system, and time of access.

Depending on the beacon implementation, some embedded applications can facilitate additional intelligence collection on the miscreant’s system. This collection can involve data exfiltration from the system, keystroke logging, and access to physical devices such as webcams. This collection can be persistent and facilitate the installation of additional software.

Beacons are triggered any time a user opens an implanted document. This OCM is indiscriminate of the targets’ national origin or geolocation. Legitimate users also trigger the beacons and the centrally-controlled server logs metadata associated with authorized systems; US government acceptable use and monitoring policies authorize this type of data collection of employees.

2.1.1 Implications for foreign targets

The most accurate statement about the use of beaconsing OCM against foreign targets is that their use is unregulated by international law. These OCM passively collect data from the affected system, pass it back to the original user and do nothing to affect the functionality of the target system. This passive collection is akin to espionage, which does not per se violate international law. The key factor is that this type of collection results in minimal degradation to the system. This analysis is consistent with *Tallinn 2.0*, where a majority consensus of the IGE believed that a beaconsing honeypot, collecting data from foreign targets, does not violate international law during either peacetime and hostilities.^[29] Part of the IGE’s reasoning is that there is a sovereign right to protect sensitive data by embedding beaconsing OCMs within sensitive documents stored within its borders. This sovereign right to protect data or code contained on a system within one’s borders is a key factor when analyzing OCM with more severe effects, as will be discussed in following sections. The IGE also found that any collection of data resulting from the beacon would constitute nothing more than cyber espionage. The collection of metadata is relatively benign, as it collects data that must be in unencrypted, plaintext form for proper transmission.

Examining the use of OCM for military purposes within the context of ongoing armed conflicts requires the application of International Humanitarian Law (IHL), which seeks to balance military requirements with the protection of the civilian populace. However, most

of the laws restricting military operations are unlikely to apply in the case of beaconing implants. Simple collection of data and subsequent computer network exploitation (CNE) does not inflict violence upon the enemy and therefore does not qualify as an “attack.”^[30] Only actions that constitute an “attack,” which require an element of violence, are subject to the targeting provisions of IHL.^[31]

Although the beacon itself does not constitute an attack, targeting cells might use the information gained from the beacon to identify military objectives for future attacks. During hostilities, malicious actors that trigger a beacon might identify themselves as a military objective if their activity triggering the OCM is determined to have a military purpose.³² Even if the malicious actor is not a uniformed member of the armed services, their military activities may, dependent on multiple factors, result in a loss of their immunity from attack under IHL.^[33]

We next consider malicious foreign actors who trigger beaconing OCMs while performing criminal acts (e.g., stealing sensitive government data for commercial gain and not for reasons related to national security). Theft of information through cyber means violates several provisions of the US federal criminal code. 18 U.S.C. §1030 prohibits the intentional access of a computer without authorization to obtain information from the U.S. Government. Additionally, 18 U.S.C. §641 covers the theft of US property and information and does not discriminate based on the sensitivity of the stolen data. Criminal theft, however, does not necessarily equate to an internationally wrongful act for which a foreign state could be held liable. The bulk of international law applies to states. However, individual actions may be attributed to a state if the individual is acting as an agent of the state or under another theory of state responsibility.^[34] Federal agencies will need to evaluate the evidence to determine whether to proceed as a counter-intelligence or law enforcement investigation, which may affect both procedural requirements and the permissibility of specific investigational tools. It is important to remember that several federal law enforcement agencies, including some belonging to the Department of Defense, may operate under both sets of authorities.

2.1.2 Implications for domestic targets

When beacons are triggered by unauthorized United States Persons (USP), domestic law, including the Fourth Amendment, the Electronic Communications Privacy Act (ECPA), and 18 U.S.C. §1030 may limit the uses of such beacons without appropriate court orders.^[35] The Fourth Amendment protects individuals against unreasonable searches and seizures by the government and applies when a reasonable expectation of privacy exists.^[36] Government systems typically provide a warning to those accessing the system that the access constitutes a waiver of the reasonable expectation of privacy.

ECPA lays further protections on privacy beyond the Fourth Amendment and requires specific types of warrants or court orders depending on the nature of the information to be accessed. Unlike the Fourth Amendment, which applies only to state actors, ECPA applies to private citizens as well. ECPA is the umbrella act for the Wiretap Act (18 U.S.C. §2511), Stored Communications Act (18 U.S.C. §2701), and Pen Register, Trap and Trace Act (18 U.S.C. §3121). Each of these acts protects different types of data in different ways, and any use of honeypots should be reviewed carefully to ensure compliance with these acts.

A significant exception common to all sections of ECPA is the service provider exception. These exceptions, such as 18 U.S.C. §2511(2)(a)(i), permit limited interception of data when service providers are engaged in activity “which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service...” If the beacon is used solely to protect the service provider’s provision of services (to include the government when acting as a service provider), then such use of beacons will be permissible. However, the use of beacons to gather content data against the miscreant necessitates appropriate law enforcement or counter-intelligence authority to proceed. State laws, which vary widely in the area of privacy, may also impact the use of OCMs domestically.

Complications limiting the use of beacons often arise from unclear technical attribution. Given that hackers can obscure the source location of their operations using technologies such as secure tunneling or virtual private networks make it difficult to determine if the actor who triggered the beaconing OCM is a USP or not. If the collection is taking place within the US, then the agency should proceed under the assumption that the individual is a USP, until credible evidence reveals otherwise.^[37]

A common criticism regarding the domestic use of honeypots by a law enforcement agency is entrapment. Entrapment is defined in Black’s Law Dictionary as “a law-enforcement officers’ or government agents’ inducement of a person to commit a crime, by means of fraud or undue persuasion, to later bring a criminal prosecution against that person”.^[38] However, the use of OCMs by themselves constitutes neither fraud nor persuasion. Rather, they are relying on the miscreant’s initiative to access a protected system illegally. Should the law enforcement agency undertake additional acts designed to prompt the miscreant into accessing the system, then entrapment may be a factor.

2.2 Inert taint within honeypots

Next, we discuss the implications of the US intentionally tainting sensitive documents and plans for physical systems such that they become inoperable or inert when built. This type of OCM includes placing a tainted copy of a sensitive plan within an organization’s network, which consists of nuanced changes to the original schematic. These changes should be hard to distinguish by anyone outside the program developer. Tainted copies and original copies should exist on segmented systems so that a miscreant cannot easily exfiltrate both versions.

A theoretical example of this OCM is a government organization hosting the schematics for next-generation stealth aircraft technology that includes a flaw which makes the objects detectable to the originating state when integrated. Another example includes the theft of munition designs that do not fire or do not detonate correctly due to an altered wiring diagram. This OCM causes a miscreant to waste money during production, tarnishes the reputation of the intelligence collector, and causes adversarial organizations to second-guess the integrity of other stolen IP.

The government actor could also couple tainted sensitive data with a beacon to improve situational awareness of offending actors. Such a combination provides a state with the option to conduct follow-on CNE against its adversary and to monitor the subsequent chain of custody for stolen sensitive data. Chain of custody is key to an intelligence agencies ability to track and observe associated actors that receive the tainted data. If not incorporated, the affected governmental entity may lose visibility on the data once it leaves the network (which subjects this OCM to many of the same limitations of other defensive techniques we identified in Section 2).

2.2.1 Implications for foreign targets

The possibility of using an OCM with foreseeably harmful effects against foreign actors raises the difficult issues of legal attribution. As used in this section, attribution refers to circumstances when a state can be held responsible under international law for the breach of an international obligation by an individual. Actions which both breach an international legal obligation (i.e., the prohibition on the use of force found in the UN Charter), and are legally attributable to a state, are known as “internationally wrongful acts.”^[39] Typically, attribution refers to situations where the actions of an individual or non-state group become the responsibility of the state. Although this issue may come up regarding OCMs, the analysis will change little from other types of cyber operations. Actions can be attributed when the effects are determined to meet the standards of causation, required to hold a state responsible. Determining this type of attribution of the effects resulting from honeypot operations is particularly difficult due to the lack of clarity of the legal standards of causation.

Under general principles of law, effects are only attributed to a cause if they meet certain specific standards of causation. Potential standards include intent, foreseeability, strict liability, and proximate causation. Unfortunately, there is no agreement under international law, either in treaty or customary law, as to which standard would apply in the context of OCMs. Whereas the harmful effects may be foreseeable, and possibly even intentional, the honeypot was not the proximate (or nearest) cause of the damage because an intervening event, the data's theft by the miscreant, had to occur for the effects to result. The *Tallinn Manual 2.0*'s discussion of honeypots reflects this uncertainty in the law. The IGE's opinion was divided, with the majority holding that no attribution would exist for the state employing the honeypot, as the affected state had to take the affirmative, albeit unintentional, the step of transmitting the

tainted files into their own system.^[40] It must be stressed, however, that this is not an issue upon which states have yet to officially comment. Until the customary law develops in this area into codified, binding law, the legal question must be considered unresolved.

Legal attribution is particularly important when discussing OCM, due to the potential of affecting unintended targets. A potential weakness of the use of honeypots is that unforeseen actors may acquire the tainted material and use them in a manner which contradicts the purposes of the employing state. It may be wise to utilize protective devices, such as self-destruct mechanisms or the ability to remotely delete the file. However, given that the result is unlikely to be legally attributed back to the originating state for the above-stated reasons, this is more a policy than a legal concern.

Another factor determining the legality of OCMs is whether a state employs the honeypot for use in peacetime or within an armed conflict. During hostilities, if a state uses a honeypot for a military purpose, then states must examine the applicability of IHL rules. One such IHL rule that applies to all military operations within an armed conflict, whether or not that operation meets the definition of an attack, is the requirement that “constant care” be taken to spare civilians and civilian objects.^[41] Although the exact meaning of constant care is difficult to pin down, the Tallinn IGE states that the duty requires “commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon.”^[42] Therefore, if it is foreseeable that a triggered OCM will affect the civilian population with no military advantage to be gained, then commanders should seek to avoid or limit these effects if possible. The general principles of humanity and military necessity support the constant care requirement as well. As stated in the DoD Law of War Manual: “A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war”.^[43]

An additional IHL obligation that potentially exists even where there is no legal attribution for an attack is the requirement, whether by treaty or by policy, to conduct legal reviews of weapons, means, and methods of warfare. A legal review examines IHL principles such as superfluous injury, discrimination, and explicitly banned arms to determine their potential compliance under IHL.^[44] More specifically under API Article 36 is the “obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party”.^[45] However, there is lack of agreement as to whether, or to what extent, the API requirement is considered customary international law. Although the US is not a party to API and has made no statement as to the customary nature of Article 36, by policy the US conducts legal reviews of weapons and, in some cases, cyber capabilities.^[46] The U.S. Air Force, for example, requires by policy legal reviews of “cyber capabilities,” defined as “any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer

systems, data, activities or capabilities”.^[47] In addition to an acquisition level legal review, all cyber operations that intend to produce effects that amount to an attack under IHL should be reviewed for compliance with targeting restrictions under IHL.^[48] For parties to the treaty, these requirements are encapsulated in API. However, many of the API rules are understood to constitute customary international law. These requirements include the rules governing distinction and proportionality.^[49]

There is much debate over what cyber effects qualify as an attack.^[50] The Tallinn Manual 2.0 definition of a cyberattack is “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”^[51] The rule is facially uncontroversial. However, what constitutes “damage or destruction” to objects is complicated by operations that cause a system to cease functioning or reduce functionality without any apparent physical damage. Whether such effects against functionality result in qualification as “damage” has yet to reach a consensus under international law.^[52]

The use of OCM whose effects would normally qualify as an attack in an armed conflict raises a bit of a paradox. Despite potential legal or policy requirements for acquisition-level legal reviews on cyber capabilities, the use of such a capability in an OCM may not require consideration of IHL targeting provisions. As previously discussed, the effects of an OCM may not be legally attributed to the originating state because it is not responsible for the transmission of the code outside its system. Furthermore, it is unlikely to be legally attributed to the state that triggered the OCM because that state would be unaware of the OCM. This lack of responsibility creates the unsettling situation where a near-total lack of responsibility exists. The only definitive legal restriction on use continues to be the requirement to take “constant care” to spare the civilian population, civilians, and civilian objects.^[53] *Tallinn 2.0* requires commanders “to be continually sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon”.^[54] As the only relevant use restriction, commanders employing these OCM should be aware that any impact on civilians is likely to be held as their moral, even if not legal, responsibility.

2.2.2 Implications for domestic targets

The potential for OCM to affect unintended domestic targets with kinetic effects, such as those resulting from an inert taint, implicates a complex array of laws affecting the domestic use of information operations. In addition to intelligence oversight laws restricting collection against U.S. persons (USPs), several federal laws and regulations limit the domestic use of information operations.^[55] An agency not operating under law enforcement, or counterintelligence authorities must be prepared to react if they receive an indication that their OCM operation has affected a USP. Depending upon the situation, this may involve cleansing procedures, termination of the operation, or handing over to an agency with the appropriate authorities. However, this would not limit criminal responsibility for the unauthorized user which accessed tainted documents on restricted government systems. If a USP is attempting

to retrieve data from a system without authorization, 18 U.S.C. §1030 is again relevant for prosecution, as well as laws restricting the gathering of national security-related information (e.g., 18 U.S.C. §793). Should that data then be traced on to an additional user, such as a foreign government, illegal disclosure laws such as 18 U.S.C. §798 may also be relevant. Furthermore, government actors, who may have authorized access to the system, are barred from illegal removal of classified material under 18 U.S.C. §1924. Two additional considerations for domestic targets are the potential for liability if the tainted documents result in damages and political blowback if the use of the tainted documents results in a threat to public safety.

2.3 Tainted honeypots for subversion

Unlike the inert taint we previously described, this OCM involves tainting sensitive data so that a cyber capability on the adverse system can become controlled by US forces when activated. Expanding upon a previous example, this OCM is possible if a government entity taints application source code embedded within a plan related to stealth technology. This new code base would allow US entities to actively change target systems, such as disrupting or outright commandeering an aircraft that utilizes the stolen intellectual property which contained the embedded code.

2.3.1 Implications for foreign targets

There is a qualitative leap with this type of OCM versus the previously described variants. Whereas the previous OCM implanted either a passive beacon or tainted documents with no further active involvement from the creating state, this type of OCM allows for active involvement in the affected system. The ability to take actions after the OCM delivers the tainted code alters the calculus under both domestic and international law. Typically, computer network exploitation against foreign computer systems by US government entities is governed by signals intelligence authorities. However, this OCM potentially involves interactive manipulation of systems for non-intelligence collection purposes, which may necessitate offensive cyberspace (or defensive cyberspace operations - response action) authorities. Conducting operations under different authorities may alter governmental oversight responsibilities, funding limitations, and approval requirements. If a foreign person or entity is the OCM target for domestic law enforcement purposes, then foreign law enforcement cooperation is typically required, most often through Department of Justice procedures.^[56]

When utilizing this type of OCM against foreign targets, there is no longer the legal attribution limitation discussed regarding passive OCM operations. If the OCM permits active involvement on the target system, such as the commandeering of a system, then the originating state becomes legally responsible for the effects that result once the state takes an active involvement in the target system. If the effects amount to an internationally wrongful act, such as interference in inherently governmental functions of another state or illegal use

of force, then the affected state could respond with actions in self-defense, take countermeasures, or demand reparations, depending on the nature of those effects. ^[57]

2.3.2 Implications for domestic targets

The use of honeypots tainted for subversion against domestic targets is governed mainly by the previously mentioned electronic privacy laws, such as the Fourth Amendment and ECPA. However, if this OCM were to also deprive a USP of their rights to life, liberty, or property, procedural due process rights will also apply. These rules are discussed in greater detail below in the Lethal Honeypots section. One legal limitation that does not apply to government agencies engaged in official government functions are the prohibitions against unauthorized access contained in 18 U.S.C. §1030. These prohibitions have exceptions for “any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.” ^[58] Depending on the investigative techniques to be employed on the target system, the “lawfully authorized” investigation will likely require a warrant or other appropriate court order to employ the honeypot and utilize the access provided by the embedded code. Although the specific requirements for a warrant and its various exceptions are outside the scope of this article, it is recommended that the language contained in the warrant application be very specific about the intended actions during the exploitation.

We here note that there is a potential legal precedent for a US non-state actor gaining remote access and control over systems belonging to US citizens without their consent. In 2012, the Microsoft Corporation leveraged the Racketeer Influenced and Corrupt Organizations Act ^[59] as the legal basis for their takedown of the Zeus family of malware. ^[60] In this operation, Microsoft gained remote control over systems infected with the Zeus malware and cleaned the infection from the systems. Microsoft claimed that the Zeus malware posed an imminent threat to the general public. It was key that a federal court blessed the operation, undertaken in cooperation with federal law enforcement.

2.4 Poisonous honeypots

In this section, we discuss the concept of intentionally developing “poisonous” honeypots. These are OCM containing embedded code with the potential to levy destructive effects, including physical destruction or lethal effects. The OCM is activated when the target seeks out, steals, and utilizes (or consumes) tainted code, data or schematics. Poisoned systems are distinct from systems infected with computer viruses, which allow malicious code to transfer to other systems when it meets various conditions through a self-replicating mechanism. In poisoned systems, the target is responsible for acquiring and ingesting the tainted information/code and then acts as the replication mechanism. This OCM becomes potentially more lethal depending upon the actions of the target system operator.

Poisonous honeypots have proven effective as an OCM. In 2004, the U.S. Government declassified a covert Central Intelligence Agency (CIA) operation involving a “poisoned” Siberian gas pipeline. The CIA allowed Soviet spies to steal tainted pipeline control software, which when installed within their pipeline control systems caused an explosion that resulted in millions of dollars in damages.^[61] The explosion occurred in a remote location of Siberia and did not harm any humans. However, it is not a stretch to imagine poisonous honeypots that could potentially result in injury or loss of life. Fast-forward to 2007, the U.S. Department of Energy conducted a proof-of-concept cyber operation against a network-connected power generator that resulted in a controlled explosion.^[62]

Poisonous honeypots in this implementation are similar to a more conventional, but controversial weapon: booby traps. The Mines Protocol and Amended Mines Protocol define booby traps as “any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act”.^[63] As pointed out in Tallinn 2.0, it is by no means certain whether and how booby traps might apply in the cyber context.^[64] Questions as to the applicability of the booby trap provisions include threshold questions such as whether code or data could constitute a “device.” Even should a poisonous honeypot be considered a booby trap, its use as such would only be prohibited in certain circumstances, such as when used with objects associated with medical or religious functions.

Should a state develop a poisonous honeypot, then it may have to pass legal review as described in the previous sections. Engineers or software developers should work together with legal experts to ensure this type of OCM can discriminate based on characteristics such as geolocation or biometric traits, for example, keystrokes.^[65] Tailoring this OCM to affect only a predetermined, legitimate target or groups of individuals also makes intentionally lethal honeypots more palatable and viable to government policymakers. A kinetic analogy for such a tailored OCM would be the use of landmines along the Korean Demilitarized Zone (DMZ).^[66] These mines are deployed in a defined and publicized area and are only intended to harm vehicles or personnel that violate known access restrictions within the DMZ.

Such an analogy leads to the following question: should and how can we effectively alert users that networks may contain intentionally lethal honeypots without the OCM losing its effectiveness? The Korean DMZ is delineated on a map and has numerous warning signs in its vicinity. It is unclear whether including honeypot warnings within electronic access consent banners would be an accurate translation within the digital realm. Additionally, the notion of “alert fatigue” renders many warning banners ineffective.^[67] Alert fatigue occurs when computer users are so inundated with innocuous warnings that serious warnings are bypassed and unobserved. Furthermore, it is unlikely that a computer hacker would heed a consent banner considering their objective completely violates any acceptable terms of use. However,

alerting a malicious actor to the presence of OCMs may achieve deterrence, or it may lead the actor to place additional scrutiny towards any stolen data. We explore the latter in more detail in Section 3.5.

2.4.1 Implications for foreign targets

The previously discussed analysis regarding state responsibility for the use of honeypots holds for potentially lethal versions as well. However, it should not be dismissed that there is a qualitative difference in the use of potentially lethal honeypots. Should the poisonous honeypot work as intended, with lethal results on a foreign target during peacetime, states may claim this result violates the Article 2(4) prohibition on the use of force. The *Tallinn 2.0* rule defining the use of force in cyberspace is relatively uncontroversial: “[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force”.^[68] This definition includes “[a]cts that injure or kill persons or physically damage or destroy objects...”.^[69] Although we have a situation where the effects would normally constitute a use of force, we are led back to the same state responsibility issue of attribution.

States should consider viewing lethal honeypot variants in the context of the entire UN charter, particularly Articles 39, 51, and 53. There is a colorable argument that the use of a lethal or physically destructive honeypot violates the overall purpose and intent of the UN Charter. Even if no Article 2(4) violation is technically found, under Article 39 the “Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken....”.^[70] The use of a poisonous honeypot, particularly one that appears out of proportion to the information or system to be protected, may be considered by the Security Council to constitute a “breach of the peace.” The *Tallinn 2.0* IGE recognized this extended obligation in their discussion of Article 2(4), postulating that “even acts that are not directed against either the territorial integrity or political independence of a state may violate the prohibition when inconsistent with the purposes of the United Nations”.^[71]

While the UN Charter does prohibit the use of force, it does permit an exception when acting in self-defense. Articulated in Article 51, it provides that “nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs....” This right is read by many states to include “anticipatory self-defense.” Although definitions of this right abound, they all include some element of immediacy.^[72] If a state employs a lethal or physically destructive OCM to protect a very narrow class of systems, such as those controlling vital elements of national security (e.g., nuclear command and control or air defense), a strong argument exists that they are acting as a self-defense mechanism. The immediacy requirement of anticipatory self-defense is met because accessing and tampering with such systems is strong evidence of another state’s intent to launch an armed attack

against the victim state, thereby permitting the use of force in self-defense. The use of honeypots to protect vital national security systems may also be permitted as a “plea of necessity.” This customary law permits a state to take actions that would normally violate international law to respond to acts presenting a grave and imminent peril.^[73] This theory would require the defended system to be an “essential interest,” and the state must narrowly tailor the OCM to only protect “grave” threats against the system.

The argument for using lethal OCMs for anticipatory self-defense does not extend to defending a nation’s critical infrastructure and key resources (CIKR). CIKR is a domestic term that states utilize to define elements essential to security, public health, economy, and its overall way of life. CIKR does not hold any strict relevance to international law, and therefore a nation cannot integrate poisonous honeypots within CIKR defenses unless the CIKR is also a target implicating one of the previously defined theories.^[74]

When viewed within an armed conflict, OCM that may potentially inflict lethal or physically destructive effects on civilians must meet the “constant care” IHL obligation. Poisonous honeypots in an indiscriminate configuration have an increased likelihood of affecting non-combatants. As previously mentioned, poisonous honeypots can be manufactured to discriminate, selectively deploying against a target based on characteristics such as geolocation or biometrics. This obligation should not be read as being overly restrictive. Even the most carefully crafted OCM has the potential to affect a non-intended civilian target, and “constant care” is not defined in IHL. Instead, it connotes a general obligation of sensitivity to the civilian populace.

2.4.2 Implications for domestic targets

The use of poisonous honeypots domestically is highly restricted. The Due Process Clause of the Fourteenth Amendment prohibits the government from taking “life, liberty, or property without due process of law.” With regards to OCM designed to cause bodily injury or death, there are few scenarios that would not violate due process protections. Likewise, restrictions on liberty, such as the ability to communicate using a networked system, requires an order or adjudication from a court. However, it is possible that poisonous honeypots designed to destroy network equipment could be employed to protect certain narrowly defined systems, such as the previously mentioned national security or CIKR examples. The due process evaluation balances individual rights with government interests and may allow taking property without due process in limited circumstances.

The U.S. Supreme Court decision *Mathews v. Eldridge* established the factors for this balancing, holding that three factors stand out: First, the right to be impinged upon by the government action; second, the risk of depriving a right in error; and third, the burden additional procedural steps would take against the government interest.^[75] Given that a honeypot normally does not allow for procedural legal steps to be taken prior to affecting the property

rights of the miscreant operator, there needs to be an overwhelming government interest that would be unduly burdened by procedural requirements. Thus the limitation to the most critical network systems. Additionally, the effects of the OCM should be limited to system damage preventing the user from further accessing or harming the critical system.

2.5 Against using OCMs

Arguments cautioning against the use of OCM include both reasons of effectiveness and potential violations of the law. On the practical side, the value of hosting tainted schematics or code within a honeypot is diminished as valuable intellectual property existing alongside the tainted data may still be extracted by the unauthorized party. The tainted portions of the intellectual property should be nearly indistinguishable from the legitimate sections, but a highly-skilled technician may detect the taint before being affected by it. Early detection provides the technician with an opportunity to patch the stolen intellectual property in such a way as to restore original functionality. Thus, the mere creation of a tainted honeypot increases the likelihood of intellectual property theft.

Using the stealth aircraft example, a malicious actor that detects tainted elements of the data could integrate the stolen technology into their aerial platforms after conducting an abbreviated development period to repair data poisoned in the OCM. Similar to the theft of the F-35 plans, the actor now has a multi-billion-dollar capability at a fraction of the US research and development costs.^[76] The U.S. Government can take additional steps to mitigate this risk such as tainting a higher percentage of the IP or embedding more active forms of malware within the document. This controversial action could cause foreseeable harm to civilians.

Furthermore, OCMs, particularly lethal variants, may unnecessarily antagonize other states to such an extent that kinetic hostilities erupt. As we discussed in Section 3.4, OCMs that cause physical damage or induce casualties may be considered a breach of the peace, if not an illegal use of force. For perspective, consider a scenario in which a state successfully exfiltrates next-generation engine technology and integrates it within a “sixth-generation” airframe. During a test run of the newly-acquired technology, the aircraft crashes into an urban area because the foreign nation embedded a poisonous OCM within the data. An individual associated with the project leaks to the press that a foreign nation was the cause of the crash. How would the state react? This scenario breaks from the steady-state game of “spy-versus-spy” in which nations regularly conduct CNE and other forms of espionage against one another.

Also arguing against the prolific use of honeypots with effects ranging beyond espionage is the immature development, particularly regarding pronouncements by states, of international and domestic law as applied to the cyber domain. For OCM under international law, whether states can be held responsible for their effects is the threshold question. Currently,

the weight of opinion is against holding states responsible for employing OCM because the act of accessing a protected system and removing the tainted code, data, or plans is carried out by the miscreant. This is particularly true of honeypots that act in a more passive manner, such as beaconing. Such acts are unlikely to rise above the level of espionage, which is not per se regulated by international law. However, if the law develops a causation standard such as intent or foreseeability, those OCM employing more potentially violent effects could, at worst, be viewed as illegal uses of force violating the UN Charter, or, at a minimum, as breaches of international norms resulting in damaged international relations. Until international law matures in this area, developers of OCM should be careful to design them to be highly discriminate and with the minimum effects required to achieve their desired ends. These steps will also aid in ensuring their use within an armed conflict complies with IHL.

Use of OCM domestically is more restricted than is the case against foreign targets and should also be given careful legal consideration. Even when employed by a government agency with the appropriate authorities, multiple areas of law restrict their use against USPs. Criminal law, privacy law, national security law, and due process considerations all limit when and how OCM can be employed domestically. Furthermore, public policy considerations such as public safety may limit the use of OCM, particularly those which may result in physical damage to objects or injury and death to persons.

3. CONCLUSION

Throughout this paper, we identify various OCM that state actors may use to complement threat modeling and other state-of-the-art defensive techniques. OCMs provide defenders with a degree of control and situational awareness that standard defenses cannot offer, especially once stolen data leaves its originating system. State actors must understand that the degree of invasiveness their OCM requires may produce drastically different legal and ethical issues depending if the OCM is (1) used during peacetime or during hostilities or (2) used against foreign actors or USPs.

The OCMs discussed in Section 2 present a possible evolution of digital defense techniques. How nations choose to implement such OCMs may alter worldwide perceptions of these techniques. These OCMs could represent the first viable cyber deterrent for protecting systems such as our nuclear command and control systems, or, these OCMs could be the antagonizing factor that triggers the next kinetic conflict. *Tallinn 2.0* briefly discusses the use of OCMs, but there is yet to develop an international norm or binding law governing their use. Nations must determine if they will proactively recognize the set of legal and ethical issues OCMs create and codify norms for their use; alternatively, if nations maintain OCMs as a clandestine defense and deal with the ramifications after the global discovery of their use. Our discussion of controversial OCMs such as poisonous honeypots does not constitute our endorsement of those tactics but is meant to trigger follow-on discussions about its place in defending sensitive intellectual property and information. 🛡️

NOTES

1. Ross Anderson et al., “Measuring the cost of cybercrime,” in *The economics of information security and privacy* (Springer, 2013), 265–300; Scott J Shackelford, “Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk,” *Chap. L. Rev.* 19 (2016): 445; Steve Mansfield-Devine, “The Ashley Madison affair,” *Network Security* 2015, no. 9 (2015), 8–16.
2. Kyle Mizokami, *The Cost of the F-35 Is Going Up Again*, 2017, accessed August 2017, <http://www.popularmechanics.com/military/aviation/a27332/f-35-rising-cost/>; Peter W. Singer, “Cyber-Deterrence And The Goal of Resilience 30 New Actions That Congress Can Take To Improve U.S. Cybersecurity,” Hearing on “Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities” Before the House Armed Services Committee, March 2017.
3. McAfee, “Estimating the global cost of cybercrime,” McAfee, Centre for Strategic & International Studies, 2014.
4. VMware, *Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon*, 2014, <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-top-five-considerations-for-choosing-a-zero-client-environment.pdf>.
5. Rory Ward and Betsy Beyer, “BeyondCorp: A New Approach to Enterprise Security,” *login: Vol. 39, No. 6* (2014): 6–11; Barclay Osborn et al., “BeyondCorp: Design to Deployment at Google,” *login: 41* (2016), 28–34, <https://www.usenix.org/publications/login/spring2016/osborn>.
6. Palo Alto Networks, *Aperture: Solution Brief*, 2017.
7. <https://www.paloaltonetworks.com/resources/techbriefs/aperture>.
8. Konrad Rieck et al., “Automatic analysis of malware behavior using machine learning,” *Journal of Computer Security* 19, no. 4 (2011), 639–668.
9. Ling Huang et al., “Adversarial machine learning,” in *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (ACM, 2011), 43–58.
10. Rock Stevens et al., “Summoning Demons: The Pursuit of Exploitable Bugs in Machine Learning,” arXiv preprint arXiv:1701.04739, 2017, <https://arxiv.org/abs/1701.04739>.
11. The Open Web Application Security Project, *Category:OWASP Best Practices*, 2017, <https://goo.gl/fvSuqX>.
12. The Open Web Application Security Project, “OWASP Top 10 2017,” *The Ten Most Critical Web Application Security Risks*, 2017, <https://goo.gl/cugAF6>.
13. GM Hardy, “Beyond Continuous Monitoring: Threat Modeling for Real-time Response,” SANS Institute, 2012.
14. Josiah ABS Dykstra and Stephen R Orr, “Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making,” in *Cyber Conflict (CyCon US)*, International Conference on (IEEE, 2016), 1–6.
15. 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 & Security Research* 1, no. 1 (2011): 80; Michael Muckin and Scott C Fitch, “A Threat-Driven Approach to Cyber Security,” Lockheed Martin Corporation, 2014.
16. Microsoft Corporation, *The STRIDE Threat Model*, 2005, [https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx); Microsoft Corporation, *Microsoft Threat Modeling Tool* 2016, 2016, <https://www.microsoft.com/en-us/download/details.aspx?id=49168>.
17. Lance Spitzner, *Honey pots: tracking hackers*, vol. 1 (Addison-Wesley Reading, 2003).
18. Meenakshi Thapliyal et al., “Botnet Detection, Measurement and Analysis: Research Challenges,” *Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering – EEC 2013*, 2013.
19. Ari Juels and Ronald L Rivest, “Honeywords: Making password-cracking detectable,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (ACM, 2013), 145–160.
20. Adel Ka, *honey*, 2017, accessed July 2017, <https://github.com/Ox4D31/honeyLambda>.
21. Roger Dingleline, Nick Mathewson, and Paul Syverson, *Tor: The second-generation onion router*, technical report (Naval Research Lab Washington DC, 2004).
22. Omar Khan, *Simple pure-python spider trap for testing crawlers*, 2014, <https://github.com/omarkhan/spidertrap>, accessed July 2017.
23. ACCESS DENIED, *DFS Issue 55*, 1996, <http://textfiles.com/magazines/DFS/dfs055.txt>.
24. Vivek Yadav, *Do not unzip this – it is a huge 42 KB file !!*, 2008, <https://techstroke.com/do-not-unzip-this-it-is-a-huge-42-kb-file/>.

NOTES

25. Laurel O'Connor, "Celebrity nude photo leak: Just one more reminder that privacy does not exist online and legally, there's not much we can do about it," Golden Gate University School of Law Review Blog, 2014, <https://goo.gl/X3b4GK>.
26. Office of the General Counsel, Law of War Manual (U.S. Department of Defense, 2016), §16.1.
27. *Ibid.*, §1.8.1.
28. *Ibid.*, §1.8.
29. The Economist, Schumpeter: Manage like a spymaster, 2015, <https://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protect-themselves-against-cyber-attacks-manage>.
29. Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), r. 93.
30. In this context, CNE is the penetration into targeted digital systems for observation and gathering intelligence data.
31. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," 1125 U.N.T.S. 3, 1977, Article 49.
32. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, r. 93.
33. *Ibid.*, r. 97.
34. International Law Commission et al., Report on the work of its fifty-third session (23 April-1 June and 2 July-10 August 2001), UN Doc, technical report (A/56/10, 2001).
35. 22 U.S.C. §6010 defines a USP as "any United States citizen or alien admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States."
36. "Katz v. United States, 389 U.S. 347," 1967.
37. LTC Barnett and A Patrick, "Domestic operational law handbook for judge advocates," US Department of Defense, Directive 3025 (2009), 170.
38. Bryan A Garner, "Black's Law Dictionary, Second Pocket Edition, St," Paul, Minn, 2001, 238.
39. Commission et al., Report on the work of its fifty-third session (23 April-1 June and 2 July-10 August 2001), UN Doc, Article 2.
40. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, r. 32, cmt. 16.
41. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," 1125 U.N.T.S. 3, 1977, Article 57(1).
42. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, r. 114, cmt. 4.
43. Office of the General Counsel, Law of War Manual, §16.5.1.
44. Office of the General Counsel, Law of War Manual, §6.2.2.
45. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," Article 36.
46. DoD Directive, "5000.01, The Defense Acquisition System," US Department of Defense. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2007, E1.1.15.
47. U.S. Air Force, "Air Force Instruction 51-402: Legal Reviews of Weapons and Cyber Capabilities (Washington, DC: GPO, 27 July 2011), 2. 24":Para 3.1.
48. Office of the General Counsel, Law of War Manual, 16.5.1.; Michael N Schmitt, "Peacetime Cyber Responses and War-time Cyber Operations Under International Law: An Analytical Vade Mecum," Harv. Nat'l Sec. J. 8 (2017): 261.
49. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," Articles 48, 51.
50. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum," 266.
51. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, r. 92.
52. *Ibid.*, r. 92, cmt. 10.
53. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts," Article 57.
54. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, r. 114, cmt. 4.

NOTES

55. Nancy Snow, "The Smith-Mundt Act of 1948," *Peace review* 10, no. 4 (1998): 619–624.
56. Nathan Judish, *Searching and seizing computers and obtaining electronic evidence in criminal investigations* (Office of Legal Education, Executive Office for United States Attorneys, 2009), 56.
57. Commission et al., *Report on the work of its fifty-third session (23 April-1 June and 2 July-10 August 2001)*, UN Doc; Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum," 244.
58. 18 U.S.C. §1030(f).
59. G. Robert Blakey and Brian Gettings, "Racketeer Influenced and Corrupt Organizations (RICO): Basic Concepts-Criminal and Civil Remedies," *Temp. LQ* 53 (1980): 1009.
60. RD Boscovich, "Microsoft and financial services industry leaders target cybercriminal operations from Zeus botnets," *The official Microsoft blog*, 2012, <https://blogs.microsoft.com/blog/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets/>.
61. Alec Russell, *CIA plot led to huge blast in Siberian gas pipeline*, 2004, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html>.
62. Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to cyber-warfare: A multidisciplinary approach* (Newnes, 2013).
63. II Protocol and II Amended Protocol, *Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices*, 1980.
64. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, r. 106, cmt. 2-3.
65. D Shanmugapriya and Ganapathi Padmavathi, "A survey of biometric keystroke dynamics: Approaches, security and challenges," *arXiv preprint arXiv:0910.0817*, 2009.
66. ELEANA J. KIM, "Toward an Anthropology of Landmines: Rogue Infrastructure and Military Waste in the Korean DMZ.," *Cultural Anthropology* 31, no. 2 (2016), 162–187, <https://doi.org/10.14506/ca31.2.02>.
67. Matthew Grissinger, "Warning! don't miss important computer alerts," *Pharmacy and Therapeutics* 35, no. 7 (2010), 368.
68. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, r. 69.
69. *Ibid.*, r. 69, cmt. 8.
70. *Charter of the United Nations*, 1945.
71. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, r. 68, cmt. 2.
72. *Ibid.*, r. 73.
73. *Ibid.*, r. 26.
74. Since a nation defines its own CIKR, a nation could simply define everything as CIKR and essentially authorize the use of force against other nations at will.
75. U.S. Supreme Court, *Mathews v. Eldridge*, 424 U.S. 319 (1976).
76. Singer, "Cyber-Deterrence And The Goal of Resilience 30 New Actions That Congress Can Take To Improve U.S. Cybersecurity."

Cultivating Technology Innovation for Cyberspace Operations

Colonel Stoney Trent, Ph.D.

“Pursuit of innovation need not require big bets on uncertain futures... [Organizations] can succeed ... by harnessing the past in powerful ways”^[1].

Our Nation and our allies are fighting a Cyber Cold War against multiple capable adversaries.^[2] Like the original Cold War, we have lost ground in the first decade by failing to acknowledge the breadth and sophistication of our adversaries’ actions. While recent hacks of financial and political institutions have drawn significant attention, some of the most disturbing intrusions have been directed at military and nuclear industries. Sadly, these cyber-attacks have been met with general inaction. Widespread Russian cyber-attacks in Ukraine^[3] set the conditions for an invasion that was generally described as a separatist movement.^[4] The most recent National Security Strategy emphasizes the gravity of China and Russia’s information operations.^[5] Unfortunately, disinformation sown about and through cyberspace attacks has resulted in domestic squabbling that has limited our ability to govern effectively, let alone mount an effective response.

Fortunately, the United States (US) and its allies have great potential to prevail again. A great legacy of the US is its ability to rebound from initial losses. As with the first Cold War, it is imperative that the government leverages the best attributes of its industrial base to enable its military to adapt and defeat emerging threats. For example, in response to growing cyber threats, the Defense Department (DoD) established U.S. Cyber Command (USCYBERCOM) in 2009 to defeat threats in and through cyberspace.^[6] The Cyber Mission Force (CMF), as illustrated in Figure 1, will eventually consist of approximately 6,200 active-duty personnel organized into 133 cyber teams.^[7]

*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 Stoney Trent is a Cognitive Engineer and Army Cyber Warfare Officer, currently serving as the Chief of Operations and Plans for the Joint Artificial Intelligence Center under the Department of Defense Chief Information Officer. Previously, he served as the Chief of Experimentation and Director of the Cyber Immersion Laboratory at U.S. Cyber Command. He has 23 years of experience in operations and intelligence assignments in tactical, operational, and strategic echelons. His research has focused on team cognition and automation support for mission command, intelligence, and cyberspace operations. He is an Army War College graduate who served as Cyber Fellow at the National Security Agency.

An additional 2,740 Reservists and National Guardsmen will augment these teams and provide another 36 teams when mobilized. [8] The Army’s portion of the CMF is 62 teams, including 11 National Guard and 10 Reserve cyber protection teams. [9] Active duty Army cyber teams are based in the National Capital Region, Georgia, Texas, and Hawaii. Army National Guard and Reserve units operate from 30 States, South Korea, and Germany. As with previous conflicts, innovation in operations, training, and technology will ensure these forces can overmatch adversaries.

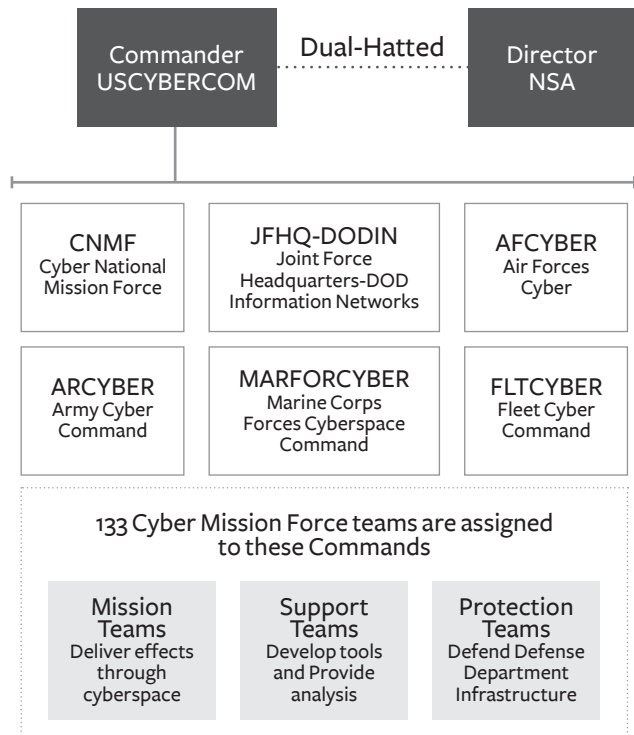


Figure 1. The Cyber Mission Force [9]

Innovation is adopting, adapting, or developing a new device, system, policy, program, process, product, or service. ^[11] Innovation permits the Army to stay ahead of determined enemies and accomplish the mission. ^[12] The Army has formally acknowledged that the pace of change in the current operating environment demands more innovation ^[13], but leaders must implement strategies and philosophies. Even the best leaders will fail to achieve a vision without the proper culture and resources. This report summarizes characteristics of previous innovation activities and offers recommendations for how the Army could cultivate technology (devices and systems) innovations for cyberspace operations.

What encourages innovation?

A cornerstone of American success has been its proclivity for innovation. Historians, sociologists, and management scientists have studied innovation activities in the US and have documented environmental, organizational, and individual commonalities in both public and private sector innovations. The preponderance of research on past innovative environments began in the 1990s with studies of regions such as Silicon Valley.

Silicon Valley is an innovative ecosystem that has been cultivated over the past century. Before the 1960s, the Santa Clara Valley was an agrarian region known as the “Valley of Heart’s Delight” because of its vast orchards and pleasant climate. ^[14] It was also the home to Stanford University, a private institution, which had been developing wireless communication technologies for the Navy since the early 1900s. ^[15] During and after World War II, Frederick Terman, the dean at Stanford’s College of Engineering, not only encouraged increased defense spending at Stanford but also emphasized partnerships with local corporations. These partnerships, through which the university shared laboratory facilities and talent with new companies, created a cycle of successful ventures and increased defense-related investment. Amongst the thousands of startups that have emerged in Silicon Valley are Hewlett-Packard, Apple, SanDisk, Facebook, Netflix, and fifty-six other Fortune 1000 companies. ^[16]

Unlike other innovation districts such as Hartford (precision manufacturing in late 1800s), Detroit (assembly line automotive construction in early 1900s), or Minneapolis-St Paul (medical technologies in 1950s), Silicon Valley has ridden consecutive waves of technology development, such as radio communications (1930s), aerospace (1950s), electronics (1970s), computing (1990s), and internet applications (2010s). ^[17] A confluence of features fueled this evolution. Foremost were loosely constrained resources in the form of substantial and sustained government research ^[18], and a world-class private university with close ties to local industry. The region has favorable weather, scenery, and immigration rules that entice talented people to live there. Entrepreneurial corporate and academic cultures encouraged risk-taking and information-sharing. Local government was supportive of technology-related development. ^[19] Aggressive venture capitalists were entrepreneurs themselves and were knowledgeable and involved with start-up activities. ^[20] Over time, the region’s dense social

networks and open labor markets allowed for talented people to move between companies as startups came, grew, or went. Many other regions have attempted to replicate Silicon Valley's success with mixed results.

AnnaLee Saxenian has extensively compared Boston, MA to Silicon Valley.^[21] She noted that prominent universities, a history of defense spending, attractive city infrastructure, and a desire to encourage technology development had placed Boston on an equal footing with Silicon Valley by the early 1980s. However, Silicon Valley companies grew by \$25B between 1986 and 1990, while Boston companies, which included Raytheon, Boston Scientific, and Digital Equipment Corporation (acquired by Compaq in 1998), grew by only \$1B. Many of the historic strengths of New England business dampened growth in the 80s and 90s. The region was dominated by highly self-sufficient companies with hierarchical organizations, vertical information flow, and centralized decision-making. Manufacturers clung to proprietary architectures and emphasized secrecy over collaboration with other companies. Vertically integrated companies (i.e., companies that handle design, manufacture, test, marketing, and support) allowed for controlled profits but hindered adaptation. Business associations focused on lobbying for legislation and tax cuts rather than industry cooperation and standard setting.

Furthermore, venture capitalists were financial professionals, rather than technologists and entrepreneurs, so they provided little more than resources and profit expectations for their ventures. Interestingly, when many Silicon Valley companies adopted New England business models in the late 70s and early 80s, they lost ground to Japanese industry. A return to principles of cooperation and collective innovation in the 80s and 90s restored their dominance.

Other regions that have attempted to recreate Silicon Valley include New Jersey, Texas, and New York. In southern New Jersey, RCA and Bell Labs attempted to set up partnerships with Princeton. RCA Sarnoff Lab exchanged researchers with the university, while Bell Labs created its own program, called the Institute of Science and Technology, to grow research talent in-house. Bell sought investments from other regional corporations as well as a partnership with Princeton. Texas companies desiring a source of engineering expertise established the Graduate Research Center of the Southwest. Southern Methodist University created the Foundation for Science and Engineering and even hired Frederick Terman as the president. The Microelectronics and Computer Cooperative and the Semiconductor Manufacturing and Technology Institutes were established in Austin. Sadly, none of these organizations were able to integrate their regional economies, which were comprised of vertically integrated companies.^[22] New York created a Center for Industrial Innovation, which was centered on Rensselaer Polytechnic Institute (RPI). Unfortunately, the Albany-Troy region lacked a strong industrial base to capture innovations, so RPI ended up exporting its best ideas and graduates to other places.^[23] Each of these efforts lacked a critical mass of defense spending and

failed to foster an ecosystem of interdependent startups like that in Silicon Valley.

Margaret O'Mara offers another contrast case in her detailed analysis of the Georgia Institute of Technology and Atlanta. ^[24] Georgia Tech is a state-funded university that was originally intended to improve industrialization in the South. As a public university, it is subject to the whims of state legislators for its financing and thus has limited incentive to encourage city economic development. This resulted in most development to support technology activities being in remote suburbs, which were disconnected from the main campus. City planners were focused on retail capacity and entertainment facilities, rather than high-tech development. Georgia Tech also did not benefit much from post-WWII defense spending. "In order to stay solvent, the school dared not stray far from its original mission - to serve the state's interests rather than greater and more intangible academic ends". ^[25] Atlanta also suffered from a history of racial intolerance and socioeconomic division that consumed political activities for decades during which major advancements were being made elsewhere. Ultimately, Georgia Tech lacked "the size, capacity, or powerful leadership to become the center of another Silicon Valley". ^[26]

Although the available historical analyses focus on the growth of innovation districts in the twentieth century, they are still instructive. Each of the previously discussed regions has undeniably matured since 2000; however, it is helpful to understand how and why they advanced at variable paces. In each case, the regional economy, culture, infrastructure, and policies were important local contributions to innovation. In effect, these factors can be thought of as the soil of innovative ecosystems.

Scientists investigating urban growth have noted interesting patterns that emphasize the importance of physical proximity. An analysis of a variety of urban development measures determined that innovation and creativity, as measured by patents and research and development jobs, follow a positive power law with scaling exponents between 1.15 and 1.27. ^[27] For example, cities that were 10x larger than other cities had 18x more inventors, and cities that were 50x larger produced 143x more patents. This exponential increase in innovation is related to social networks and access to ideas, resources, and expertise in more populated urban settings. Transaction costs are lower in more densely packed cities. Local hiring is more comfortable, and experts find it easier to move between organizations. Serendipitous exchanges are more likely as experts from various industries interact socially. Of note, the degree of success captured from this scaling is reduced in districts that suffer from too much control of information. ^[28] This appears to explain why populous cities across Asia have failed to recognize innovative successes commensurate with their size. Additionally, prosperous regions benefit from organizations prepared to sow and nurture the seeds of innovation.

Individualistic societies, such as the US, tend to emphasize the role of individual experts in innovative outcomes. However, recent research challenges the notion that lone geniuses are

the prototypical innovators. Andrew Hargadon advances a network perspective that suggests innovators are not necessarily smarter, but rather more connected than others.^[29] This has important implications for how organizations enable innovation. While specialized talent is important, information sharing may be more so. Hargadon's analysis of technology innovations from Edison's Menlo Park to Ford's factory floor and Jobs' garage suggests that most innovations are recombinations that combine existing objects, concepts, and people in ways that spark technological revolutions. Such brokering involves spanning industries, moving ideas and building new communities. "Hiring smart people, building flat organizations, and cross-functional teams, and engaging in brainstorming and rapid prototyping are not enough to make organizations innovative".^[30]

Innovative organizations and ecosystems include a core of specialists as well as a cadre of generalists responsible for spanning and brokering. Spanners are not liaisons, but rather people with (or willing to develop) first-hand experience in multiple domains. Lawyers in Silicon Valley have historically played such a role.^[31] Lawyers have exposure, access, and trust amongst many companies and serve as connective tissue in and between industries. They can mediate crucial flows of resources and information and facilitate the consolidation and legitimization of ideas and organizations. McKinsey and Company, a global management consulting firm, not only brokers information between industries but also maintains its own "Rapid Response Team," which is responsible for connecting internal experts for projects.^[32] Spanners maintain weak links to spark ideas and connect experts who subsequently build strong links to capture them. Workspaces encourage or discourage these linkages.

More attention is being paid to how workgroups are impacted by their workspaces. Innovation workplaces require a balance between order and chaos.^[33] Open office plans afford no privacy, and closed offices discourage coordination. Cross-fertilization and interdisciplinary work require ample space to exchange ideas, while private spaces are needed for seclusion and reflection. Telework reduces overhead and offers individual flexibility but reduces opportunities for employees to intermingle. Because intermingling is critical for recombination, it is no surprise that successful, high tech organizations still invest in workspaces that promote face-to-face interactions.^[34] Ultimately, workplaces must be flexible and tailored to the current work needs of the workgroup. "Cookie-cutter settings will produce cookie-cutter ideas."^[35] MIT's Building 20, now replaced by the Stata Center, was a World War II-era temporary structure that afforded great flexibility during its fifty-year existence, cultivating efforts as diverse as the first hackers, Noam Chomsky's linguistics department, and Bose Acoustics and Digital Equipment Corporation.^[36] Microsoft's Redmond Lab, or Building 99, is similarly built to be reconfigured with little effort.^[37] Such flexibility is critical in light of the finite lifespan (approximately twenty years) of innovation districts, spaces, or groups.^[38]

Organizational behavior research has identified a wide variety of factors that are common amongst innovation activities. A meta-analysis of 46 studies conducted between 1960

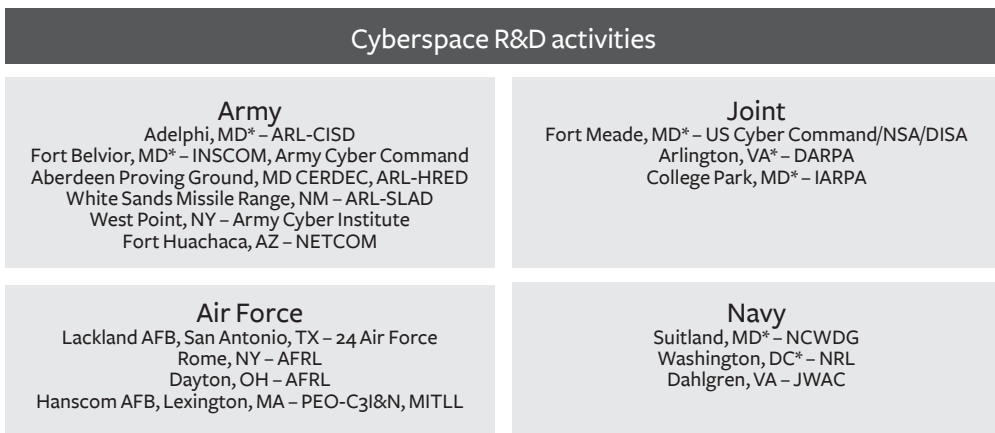
and 1988 found that specialization, managerial attitude toward change, slack resources, and communication were associated with innovation. ^[39] A more recent meta-analysis of 133 studies of public sector innovation between 1990 and 2013 revealed that slack resources, leadership styles, incentives with clear goals, low-risk aversion, and employee autonomy were common across innovative activities. ^[40] A survey of Australian Public Service Commission employees showed that experimentation, corrective action for low-performers, feedback loops, and motivation to make improvements enhanced the likelihood of innovative activities. ^[41] An analysis of over 96,000 responses to a Canadian workplace survey between 1999-2006 found that highly qualified personnel, motivated employees with consistent opportunities to innovate, and innovation as a persistent strategic priority contribute to innovation. ^[42] A Smithsonian Institute study determined that charismatic leaders who were supportive of individual researcher freedom and interdisciplinary teamwork were common amongst US places of innovation. ^[43] Examples of individual autonomy can be found at Google and 3M, where they direct their engineers to allocate fifteen to twenty percent of their time to pursue projects of their interest. ^[44] Employees are only required to provide regular updates to their supervisors on their initiatives. These studies provide compelling insights into individual and organizational contributions to innovations. Table 1 summarizes them alongside the previously discussed environmental characteristics to suggest ways for the Army to encourage innovation.

| Environmental | Organizational | Individual |
|---|---|---|
| Inter-organizational relationships | Slack resources | Specialization/Highly qualified personnel |
| External pressures | Feedback loops | Employee autonomy |
| High density employment pools | Experimentation | Charismatic, supportive leader |
| Appealing locale (weather, outdoor activities, scenery) | Communication | Motivation for improvement |
| Successful regional economy (schools, businesses, public transportation) | Incentives with clear goals | Corrective action for low performers |
| Favorable immigration rules | Interdisciplinary work | |
| Top-tier research universities | Low risk aversion | |
| Open culture and labor markets | Mix and collaborative and private spaced | |
| Finite lifespan (~20 years) | Flexible workspaces | |

Table 1 . Characteristics of Innovative Activities

How is the Army postured for technology innovation?

Although regional characteristics are important for technology innovations, the Army has limited input over the location of its installations and major activities (basing decisions are made by Congress, but at the request of the DoD). Because of decades of base realignments and closures, most military research and development for cyberspace capabilities occurs in regions that lack the environmental elements that have been associated with technology innovation. (Figure 2 identifies the current locations of the most significant military cyberspace research and development activities.) It is unsurprising that the Army has struggled to hire highly qualified scientists and engineers in these locations. Doctoral scientists and engineers in the Army’s Research, Development and Engineering Centers have comprised between two and five percent of their workforces for decades. ^[45] As of 2007, Army Research Laboratory (ARL) had improved their doctoral workforce from twenty-five to thirty-five percent over the preceding decade, but that was far below the fifty percent for Navy Research Laboratory (both are in or near Washington, D.C.).



*Within the National Capital Region

Figure 2. Current cyberspace R&D activities and locations

A notable exceptional region is the National Capital Region (NCR). Due to the preponderance of government research activities located within fifty miles of Washington, D.C., the NCR has emerged as a new technology innovation district. With extensive federal installations as well as government-leased facilities throughout the Capital Area, there continues to be significant room for further growth. Elsewhere, the Defense Department has made poor use of military installations that are located within innovative districts. Moffett Air Field in Silicon Valley, Fort Devens near Boston, and Fort Hamilton in New York City could be software development and data science hubs but have been left fallow.

The Army has decided to move its Cyber Headquarters away from the NCR to Fort Gordon, GA. Several good reasons for this move include geographic distribution of national security capabilities, the presence of an existing military schoolhouse (the Army Signal Center), and the presence of a national cryptologic center (NSA/CSS Georgia).^[46] Additionally, inexpensive housing, power, workspace, and cooling contributed to the decision.^[47] It is likely that the colocation of training and operational organizations will encourage innovative practices in both. The seclusion of Fort Gordon may also help protect operational innovations from adversaries. Unfortunately, Augusta, GA lacks most of the characteristics that have attracted technologists to other innovation regions. Limited public infrastructure and services, sparse employment options, a humid subtropical climate, a lack of a private research university, and distance from urban centers will likely delay the emergence of innovative technologists in Augusta-Richmond County. Furthermore, technology innovations face other self-imposed constraints.

Organizations and processes stifle technology innovation in the Army. Congressionally mandated acquisition processes are implemented in a way that diffuses responsibility across large bureaucracies. For example, a cyberspace need is supposed to be identified by operational commanders (Army Cyber Command), documented by a capability manager (Cyber Center of Excellence), validated by a force manager (Army Capabilities Integration Center, G-8, and/or J-8), funded through a 5-year budget cycle overseen by a resource manager (G-8), researched by a program officer (Army Research Laboratory and Communications Engineering Research Development and Engineering Center), developed and delivered by program manager (Program Executive Office), tested by a test engineer (Army Test and Evaluation Center), and used by cyber team members.^[48] This baton passing crosses up to ten general offices, with most of the staff work and decision-making performed by people with little technical knowledge and who will never be impacted by their decisions. This convoluted and inefficient process ensures that any technology “solution” is poorly fit, or obsolete, if/when it is delivered.

Army scientists and engineers are hardworking and well-meaning, but the Army is failing them. Due to the location of Army research activities, very few scientists and engineers have access to the operators and analysts who will have to use the technologies under development. Many research program officers have limited knowledge of the daily tasks and work conditions of cyber teams. They must rely on wordy, and poorly described, requirement documents to provide critical information about users’ needs. This problem is worse for the thousands of contracted scientists who rely on the program officer for guidance. High-level research guidance gets implemented across many organizations with little coordination among stakeholders. Figure 3 illustrates the assortment of Army organizations that are conducting research and development for cyberspace capabilities. In fact, Figure 3 fails to fully capture the diffusion of cyber research within these organizations, as individual research-

ers pursue cyber and non-cyber projects. The current construct limits the pooling of highly qualified personnel and resources necessary to create slack, or flexibility, for innovation. It also makes directing and collaborating with operational units, USCYBERCOM, other Service Departments, industry, and foreign partners exceedingly difficult.

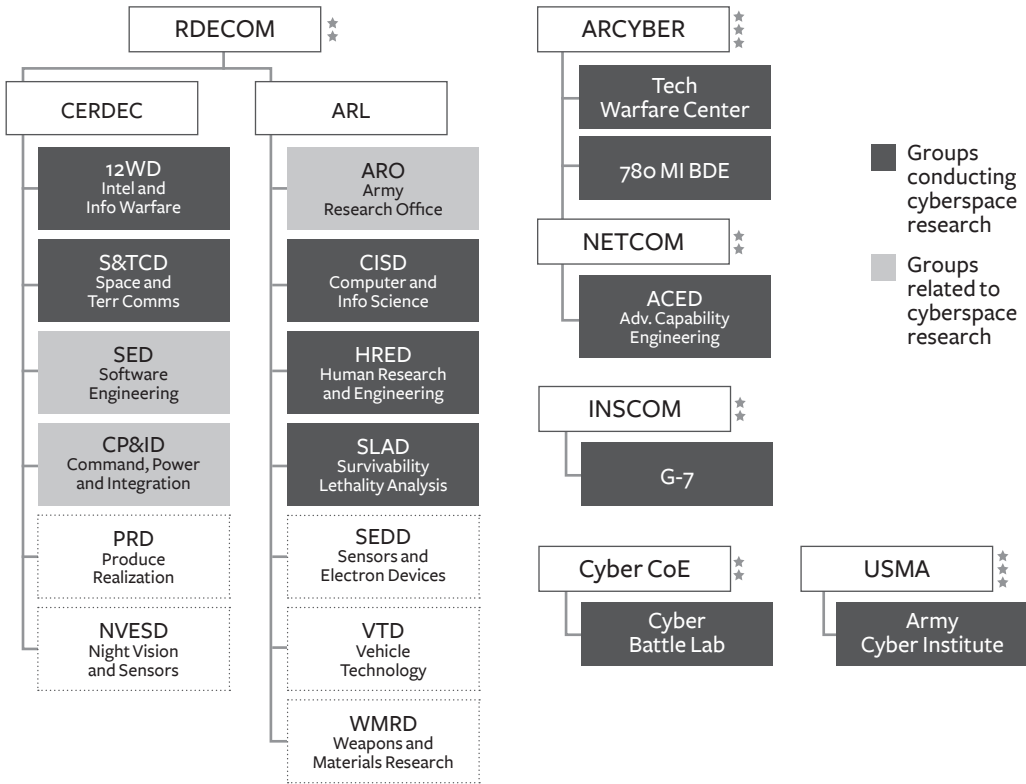


Figure 3. Cyberspace R&D within the Army^[49]

The Army has long desired more STEM talent; however, it has not fully utilized its existing talents. Assignments rarely consider academic credentials and very few personnel authorizations explicitly identify advanced degree pre-requisites. Outside of the United States Military Academy, officers are responsible for generalist staff or command roles that require no STEM expertise. As a result, officers with a Ph.D. find few opportunities outside of USMA to maintain currency and provide benefit to the Army for their graduate educations.

In 2011, former Defense Secretary Robert Gates encouraged new Army Lieutenants to seek out broadening assignments that were “off the beaten path, if not a career dead end,” and stated that the Army should encourage the effort.^[50] He was arguing for breadth and a collaborative disposition to complement depth of skill. Successful innovative corporations

foster just such a balance. ^[51]In 2012, the Defense Science Board recommended that the Service Departments make opportunities for troops to serve in laboratories and research program offices. ^[52]In 2013, the Army Science Board recommended re-establishing a military scientist and engineer career path that would direct and strengthen Army research and development. ^[53]The Army Research Development and Engineering Command (RDECOM), with the concurrence of its higher headquarters, the Army Materiel Command, attempted to implement this recommendation, but the pilot stalled out due to lethargic human resource processes. ^[54]In particular, no career incentives existed to justify individuals accepting the risk of such assignments. Additionally, assignment officers lacked the mandate to identify and adequately utilize advanced STEM skills. Unfortunately, the Army's human resource system is designed to reward successful completion of well-established roles and discourage/disadvantage innovative, new roles. Officers following Secretary Gates's recommendation will not last long in the inventory.

The recently established cyber warfare branch offers promise for niche specialists if they are not blunted by the human resource system. Army Pamphlet 600-3 now describes a career path for cyber warfare Soldiers that suggests gainful employment for the growing force. However, like cyberspace itself, personnel requirements will change more rapidly than the current human resource system can support. For example, in 2009 the DoD hastily developed a plan for the size and composition of the CMF. This plan sacrificed commanders and staff for team-level structure, forcing units like the Cyber National Mission Force and the Cyber Protection Brigade to employ a variety of workarounds to satisfy critical command and staff roles. This situation has persisted through 2018.

Although the Cyber Center of Excellence has diligently worked to update force structure documentation, it is hard to see how it will keep up with emerging operating concepts. Under the current system, validating a new requirement takes at least twelve to twenty-four months. Once a requirement is validated, assignment cycles limit the speed at which new requirements are filled. This sclerotic process results in lost opportunities and expertise as blunted innovators seek more supportive sources of employment. Although much of the current cyber branch is under initial service obligations, the insatiable demand for software developers, cyber operators, analysts, and data scientists across the Service Departments, the intelligence community, and commercial sectors will make retention difficult in the near future. Focus groups and sensing sessions will be insufficient to retain innovative experts in the force. Without an agile personnel system that can offset the private-sector advantages, our cyber workforce will become a routinized harbor for mediocrity, incapable of defeating more agile adversaries.

Recommendations for improvement

The Army recently established the Army Futures Command to dramatically improve the way in which capabilities are delivered to the force.^[55] This new Command is not a startup, but rather a merger of multiple large bureaucracies, each with its own infrastructure, heritage, and culture. As strategic integration unfolds for this Command, some proofs of concept that demonstrate the value of the new organization will be important. The sense of urgency and relatively low cost of cyberspace capabilities suggest that cyberspace capability reform would be an ideal first step. The following four recommendations fully support the intent of this new Command and can be implemented now.

Establish a Cyberspace Operations Research and Development (R&D) Group – To reduce the diffusion of responsibility and create slack resources for innovation, the Army should consolidate R&D of cyberspace capabilities as illustrated in Figure 4. The director of this group should be an academically qualified (STEM Ph.D.) cyber Colonel, with the responsibility and resources for ensuring that R&D is operationally aligned and responsive to environmental changes. The director would report to the Commander, RDECOM, and coordinate with cyber brigade commanders and the Cyber Capability Manager to exchange information about the trajectory of science and technology.

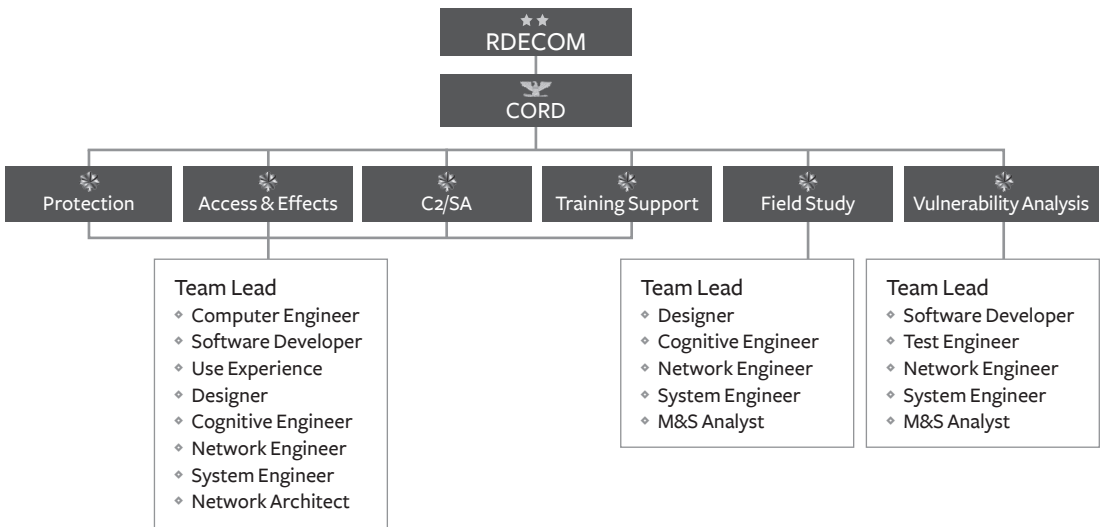


Figure 4. Army Cyberspace Operations Research and Development Group

This group should be organized into interdisciplinary research teams, each led by academically qualified cyber officers and aligned with operational requirements (performance of this organization should be measured based on operational feedback from users). Government civilians would provide continuity for this organization by serving as research

staff, project leads, and deputies. Following Title 5 of the U.S. Code and DoD policy, the Army could hire Highly Qualified Experts for up to five years to serve as technical directors in this organization. ^[56] These technical directors would provide sustainable exchanges of eminent experts from industry and academia. Because of its critical mass of technical expertise, this organization would represent cyber equities in the cross-functional teams within the Army Futures Command.

This organization should be principally located at Fort Meade and Adelphi, MD to provide it with direct access to cyber teams and the preponderance of cyber research expertise located within the NCR. To sustain appropriately skilled leaders, mid-career officers should be afforded Advanced Civil Schooling with utilization tours in this organization. In this way, select cyber officers could progress from cyber team members to cyber research leaders to cyber staff officers and return to cyber research leadership roles throughout their career. Such a program and organizational construct could be extended to other capability areas (e.g., intelligence, communications, and armaments) as well. Ultimately, the DoD would benefit from each of the Service Departments establishing a similar organization.

Improve Collaboration – The Army needs better formal and informal coordination to enable innovation. Innovation is a process in which the phased application of expertise is important. ^[57] Highly qualified scientists and engineers are critical for research phases, whereas legal, contracting and doctrine expertise are critical for implementation. In large organizations, it is difficult to locate appropriate expertise, and senior leaders have little visibility on how expertise is being applied to large-scale, complex problems. Research in cognitive psychology suggests that Transactive Memory Systems are essential for high performing organizations.

Transactive Memory Systems distribute knowledge and skills across people and tools to achieve high efficiencies. Transactive Memory theory emerged from studies of intimate couples where knowledge was efficiently federated between the two individuals ^[58] (it is more efficient for a couple to ask each other for information than for both people to know the same things). Accurate transactive memory has been observed to be a significant predictor of team performance. ^[59] In new product teams, transactive memory has positive impacts on team stability, familiarity, interpersonal trust, team learning, and effectiveness. ^[60] Support for transactive memory should include automation as well as human boundary spanners. A transactive memory support tool would analyze computer work to infer skills amongst workers. These data along with self- and colleague-reported information about skills could generate navigable knowledge graphs to help with expertise location. A dedicated knowledge management team should maintain not only this support tool but also foster inter-divisional collaborations. These informal methods will enable the actions and decisions from more formal venues.

The Army should establish or request three cyber capability councils—Army, Joint, and Combined—to plan and collaborate with other relevant organizations. The Army’s cyber capability council should be chaired by an SES or Brigadier General on the Army Cyber Command Staff and should include the following roles:

- ◆ Director, Cyberspace Operations R&D Group
- ◆ Commanders, Cyber Brigades
- ◆ Cyber Capability Manager
- ◆ Director, Army Cyber Institute
- ◆ Director, Cyber Battle Laboratory
- ◆ INSCOM G-7

The Joint Cyber Capability Council should be chaired by a Senior Executive in U.S. Cyber Command Capabilities Development Group and include all Service Cyber R&D leads and the Defense Advanced Research Projects Agency Information Innovation Office Director. U.S. Cyber Command is currently working with the Joint Staff to establish a Cyber Functional Capabilities Board (FCB) for the Joint Requirements Oversight Committee. This will be a critical coordinating body for large-scale requirements. However, most cyber capabilities will not meet the threshold for consideration by the Cyber FCB, so the Joint Cyber Capability Council should tend to the smaller scale requirements. The Combined Cyber Capability Council should be chaired by the Office of the Undersecretary of Defense for Research and Engineering, USD(RE), and include U.S. Cyber Command, the Service Cyber R&D leads and select foreign partner R&D groups (e.g., Defense Science and Technology Laboratory, Government Communications Headquarters, Australian Signals Directorate). These coordinating councils will help inform operational planning as well as avoid (or validate) redundancy and gaps in technology development.

Commit to a Campaign of Field Study and Experimentation – Field studies provide thorough descriptions of operational needs that far surpass the fidelity and consistency of After Action Reviews (AARs) and needs statements. Field studies also provide the insights necessary for the design and conduct of experiments and afford cyber teams a voice in the requirements process through the performance of their regularly assigned duties. Experimentation offers a way to democratize technology decisions, as cyber team members provide data on tool and team performance as participants. Because of the pace of change in cyber work, these complementary research activities must be a sustained campaign rather than a collection of discrete yearly projects. The research staff should be responsible for publishing unclassified findings whenever possible. In this way, academic and industry developers will be more knowledgeable of technology requirements.

USCYBERCOM has established the Cyber Immersion Laboratory, which is developing and assessing capabilities for the CMF.¹⁶¹ To date, it has been minimally staffed and resourced, with nearly all of USCYBERCOM's research funding going to external performers. The Army Cyber Center of Excellence has relabeled the Signal Battle Lab to be the Cyber Battle Lab and has been building the capability to conduct experiments to inform the cyber requirements process. These labs require a sustained budget and sufficient, appropriately skilled staff to be successful. ARL, particularly the Human Research and Engineering Directorate, should be leading or participating in this campaign to ensure that human factors are preeminent in the design of new technologies. In addition to lab staff and infrastructure, successful experimentation requires practitioners to participate.

Now that the CMF is fully operational, cyber teams should be apportioned to these laboratories as an experimentation force. Cyber battalions should designate a Chief Technology Officer who would be responsible for managing the teams' participation in field studies, experiments, and technology-oriented focus groups. In this way, the CMF can formally involve all cyber teams in a manner that accommodates collaborative planning and resourcing. Multi-domain experiments should be facilitated by including cyber teams in command post exercises and combat training center rotations. Instrumenting cyber teams to provide tool and team performance data from training and real-world operations will improve our understanding of what works and why. Ultimately, data from experiments and real-world operations will inform models that can be used to evaluate strategic and operational planning as well as technology development decisions.

Leverage existing and spawn new innovation districts – The military has been exploring ways to improve access to the knowledge, skills, and technologies in our mature innovation districts. The Defense Innovation Unit (DIU) is one example that has been focused on Silicon Valley and Boston. Other regions, such as the NCR, Pittsburgh, Seattle, Austin, and Denver are emerging as technology hubs. The Army's Futures Command has selected Austin as its headquarters to afford efficient access to that region's expertise. Despite improvements in coordination technologies, proximity and personal interactions will continue to reap the most from our existing innovative regions.

Unfortunately, the current innovation ecosystems are failing to satisfy the Nation's needs for cyber operators, software developers, and data scientists. Incremental increases to investments in established regions will recognize diminishing returns as costs of living increase. Innovation districts must be grown to dramatically increase the breadth and depth of intellectual capital, which is crucial for success in future conflicts. Because regional change is slow, wise investments in fertile locales are warranted.

Three regions offer great promise for new innovation districts—South Bend, IN, Nashville, TN, and St Louis, MO. Each region has a world-class private research university (University of Notre Dame, Vanderbilt University, and Washington University, respectively) without a federally funded or university-affiliated research center. They are in, or near, attractive cities with strong growth potential and an ability to capitalize on technologies that are developed there. They offer low costs of living and are within a two-hour flight of the preponderance of cyber teams. If these universities and their local communities are willing to partner to foster cyber or data science-related business development, the Undersecretary of Defense for Research and Engineering should establish University Affiliated Research Centers at each. These centers will accommodate broader involvement from each university and underpin the growth of more innovative ecosystems.

SUMMARY

The Cyber Cold War is raging, and the United States has the most to lose. Although the CMF is now fully operational, it will require continual technology advancements to stay ahead of our adversaries. Unfortunately, much of the Army's R&D enterprise is not well-positioned to leverage our Nation's strengths, nor is it proximal to operational practitioners. A consolidated, operationally-oriented cyberspace R&D group could afford the organizational and individual enablers of innovation while helping the Army to better utilize the talent and resources that it already has. Collaborative technologies and organizational design in the Futures Command can help the Army leverage its size with improved interconnectedness.

Improving technology innovation is critical and will not come without cost and effort. Much work is needed to set environmental conditions and organizational design to support individual initiatives. Fortunately, the DoD currently stands to benefit from increased defense spending in FY19. The Secretary of Defense fully understands the need for dramatic improvement, and fifteen years of Army acquisition failures have created the crisis necessary for change. The Secretary and Chief of Staff of the Army have initiated a generational opportunity to improve innovation. This confluence of conditions is as supportive as it is ephemeral. Without immediate, bold action, the Army will miss its best opportunity to seize the initiative in the current Cyber Cold War. Decades of studies indicate the importance of a culture of experimentation. While our adversaries are experimenting, we must not dither.

DISCLAIMER

This paper reflects the views the authors. It does not necessarily represent the official policy or position of Department of Defense, U.S. Army War College or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

ACKNOWLEDGMENT

I would like to thank Dr. Eric Hintz, with the Smithsonian Museum of American History, for his work on the History of Innovation Centers in the United States, which inspired much of the thought in this report. Additionally, General Paul Nakasone, Lieutenant General Stephen Fogarty, Lieutenant General (Retired) Edward Cardon, Colonel James Raftery, Lieutenant Colonel James Doty III, Giorgio Bertoli and other Army colleagues provided invaluable consultation. 🇺🇸

NOTES

1. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003), xii.
2. Stoney Trent, “Amid a Cyber Cold War, is the Cyber Mission Force Prepared?”, *Bulletin of Atomic Scientists*, October 30, 2017, <https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-prepared11233>.
3. Andy Greenberg, “How an entire nation became a test lab for cyberwar”, *Wired*, June 20, 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
4. Damien Sharkov, “Putin claims Russia ‘Forced to defend’ Ukraine separatists”, *Newsweek*, October 12, 2016, Accessed at: <http://www.newsweek.com/putin-claims-russia-forced-defend-ukraine-separatists-509281>.
5. National Security Strategy, United States of America, December 2017, Washington, DC.
6. Secretary of Defense (2009). Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. Washington, D.C. , June 23, 2009.
7. Stoney Trent, “Amid a Cyber Cold War, is the Cyber Mission Force Prepared?”, *Bulletin of Atomic Scientists*, October 30, 2017, <https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-prepared11233>.
8. S. Zuehlke, Status Update to RFPB Report “DoD Cyber Approach: Use of the National Guard and Reserves in Cyber Mission Force”. Reserve Forces Policy Board, Department of Defense. Washington, D.C., January 27, 2017.
9. U.S. Army Cyber School, “Cyber Career Field / Branch 17 Overview,” January 4, 2018.
10. Stoney Trent, “Amid a Cyber Cold War, is the Cyber Mission Force Prepared?”, *Bulletin of Atomic Scientists*, October 30, 2017, <https://thebulletin.org/amid-cyber-cold-war-cyber-mission-force-prepared11233>
11. adapted from Richard Daft, “A dual-core model of organizational innovation”, *Academy of Management Journal* 21, 1978, 193–210.
12. Department of the Army, “The U.S. Army Operating Concept: Win in a Complex World,” Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, October 31, 2014.
13. Department of the Army, “Army Innovation Strategy”, Office of Business Transformation, 2017.
14. Margaret Pugh O’Mara, *Cities of Knowledge: Cold War Science and the Search for the Next Silicon Valley* (Princeton, 2005), 101.
15. Martin Kenney, ed., *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, ed. Martin Kenney. Stanford (Stanford University Press, 2000).
16. <https://www.geolounge.com/fortune-1000-companies-list-for-2016/>.
17. Margaret Pugh O’Mara. “Don’t Try This at Home: You Can’t Build a New Silicon Valley Just Anywhere.” *Foreign Policy* 181, September/October 2010.
18. Stuart W. Leslie, “The Biggest ‘Angel’ of Them All: The Military and the Making of Silicon Valley,” in Kenney, *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, (Stanford University Press, 2000), 48–67.
19. Stuart Leslie and Robert H. Kargon. “Selling Silicon Valley: Frederick Terman’s Model for Regional Advantage.” *The Business History Review* 70, Winter 1996.
20. AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Harvard, 1994).
21. Ibid.
22. Stuart Leslie and Robert H. Kargon, “Selling Silicon Valley: Frederick Terman’s Model for Regional Advantage.” *The Business History Review* 70, Winter 1996.
23. Stuart Leslie, “Regional Disadvantage: Replicating Silicon Valley in New York’s Capital Region”, *Technology and Culture*, 42(2), April 2001, 236-264.
24. Margaret Pugh O’Mara, *Cities of Knowledge: Cold War Science and the Search for the Next Silicon Valley* (Princeton, 2005).
25. Ibid, 186.
26. Ibid, 222.
27. Luis Bettencourt, Jose Lobo, Dirk Helbing, Christian Kuhnert, and Geoffrey West, “Growth, innovation, scaling and the pace of life in cities”, *In the Proceedings of the National Academy of Sciences*, 104(17), April 2007, 7301-7306.
28. Steve Johnson, *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010).
29. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003).
30. Ibid, 51.
31. Suchman, 71-91.

NOTES

32. Andrew Hargadon, *How Breakthroughs Happen: The Surprising Truth About How Companies Innovate* (HBR Press, 2003), 149.
 33. Johnson, Steve. *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010), 62.
 34. Arthur Molella, "What makes an Innovative Lab or Workspace?" *American heritage of invention and technology*, Vol 25, Spring 2010, 28-37.
 35. Ibid, 29.
 36. Stewart Brand, *How Buildings Learn: What happens after they're built*, (Viking, 1994).
 37. <https://www.microsoft.com/en-us/research/lab/microsoft-research-redmond/>
<http://www.amusingplanet.com/2009/10/inside-microsofts-office-at-redmond.html>.
 38. Arthur Molella, "What makes an Innovative Lab or Workspace?" *American heritage of invention and technology*, Vol 25, Spring 2010, 28-37.
 39. Fariborz Damanpour, "Organizational Innovation: A meta-analysis of effects of determinants and moderators", *Academy of Management Journal*. 34(3), September 1991, 555-590.
 40. Hanna De Vries, Victor Bekkars, and Lars Tummers, "Innovation in the Public Sector: A systematic review and future research agenda", *Public Administration* 94, Issue 1, March 2016, 146-166.
 41. Mehmet Demircioglu and David Audretsch, "Conditions for innovation in public sector organizations", *Research Policy* 46(9), 2017, 1681-1691.
 42. James Chowhan, Fred Pries, and Sara Mann, "Persistent innovation and the role of human resource management practices, work organization, and strategy", *Journal of Management and Organization*, 23(3), 2017, 456-471.
 43. Arthur Molella, "What makes an Innovative Lab or Workspace?" *American heritage of invention and technology*, Vol 25 (Spring 2010), 28-37.
 44. Steve Johnson, *Where Good Ideas Come From: The Natural History of Innovation* (Riverhead, 2010), 93.
 45. Gilbert Decker, et al., *Improving Army Basic Research: Report of the Panel on Future Army Laboratories*, RAND Corporation, Santa Monica CA, 2012.
 46. Interview with LTG Edward Cardon, former Commander of Army Cyber Command, January 24, 2018.
 47. Email from LTG Paul Nakasone, Commander of Army Cyber Command, April 9, 2018.
 48. Department of the Army, "How the Army Runs: A senior leader reference handbook", U.S. Army War College, 28 August 2015, Carlisle PA.
 49. Compiled from interviews and personal experiences of the author.
 50. Secretary of Defense Robert M. Gates. Speech at West Point on February 25, 2011.
 51. Morten Hansen, "IDEO CEO Tim Brown: T-shaped Stars: The Backbone of IDEOs Collaborative Culture", Chief Executive, (January 21, 2010), https://chiefexecutive.net/ideo-ceo-tim-brown-t-shaped-stars-the-backbone-of-ideoes-collaborative-culture__trashed/.
 52. Defense Science Board, Report of the Defense Science Board on Basic Research, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington DC, February 2012.
 53. Department of the Army, "The Strategic Direction for Army Science and Technology", Army Science Board, Washington, DC, February 2013.
 54. Director, U.S. Army Research, Development and Engineering Command, "Authorization for the Officer Scientist Engineering Program (OSEP) Pilot", April 2013.
 55. Mark Esper, "General Orders No 2018-10: Establishment of the United States Army Futures Command", Headquarters, Department of the Army: Washington, DC, June 4, 2018.
 56. Undersecretary of Defense for Personnel and Readiness, "Revised Policy Guidance – Hiring of Highly Qualified Experts (HQEs)", Washington, DC, March 26, 2010.
 57. Fariborz Damanpour, Marguerite Schneider, "Phases of Adoption of Innovation in Organizations: Effects of Environment, Organization and Top Managers", *British Journal of Management*, 12(3), (September 2006), 215-236.
- Lisa Daniel, Patrick Dawson, "The sociology of innovation and new biotechnologies," *New Technology, Work and Employment*, 26(1), February 25, 2011, 1-16.

NOTES

58. Daniel Wegner, Toni Giuliano, Paula Hertel, “Cognitive Interdependence in Close Relationships”, In: Ickes W. (eds) *Compatible and Incompatible Relationships. Springer Series in Social Psychology*. (1985) Springer, New York, NY, 253-276.
59. JR Austin, “Transactive memory in organizational groups: the effects of content, consensus, specialization, and accuracy on group performance”, *Journal of Applied Psychology*, 88(5), October 2003, 866-78.
60. AE Akgün, JC Byrne, H Keskin, and GS Lynn, “Transactive memory system in new product development teams”, *IEEE Transactions on Engineering Management*, 53(1), February 2006, 95-111.
61. Stoney Trent, Robert Hoffman, Scott Lathrop, “Applied Research in Support of Cyberspace Operations: Difficult, but Critical”, *The Cyber Defense Review*, May 2, 2016.

THE CYBER DEFENSE REVIEW

◆ RESEARCH NOTE ◆

Supremacy by Accelerated Warfare through the Comprehension Barrier and Beyond: Reaching the Zero Domain and Cyberspace Singularity

Dr. Jan Kallberg

*“In The Land Of The Blind, The One-Eyed Man Is King.”
Erasmus Of Rotterdam, 16TH Century*

INTRODUCTION

It is questionable and even unlikely that cyber supremacy could be reached by overwhelming capabilities manifested by stacking more technical capacity and adding attack vectors. The alternative is to use time as the vehicle to supremacy by accelerating the engagements’ velocity beyond the enemy’s ability to target and precisely execute and comprehend the events as they unfold. The space created beyond the adversary’s comprehension is called the Zero Domain. Military strategists traditionally see the battle space as land, sea, air, space, and cyber domains. When fighting a battle beyond the adversary’s comprehension, the conflict occurs in the Zero Domain, not in a traditional warfighting domain.

In the Zero Domain, cyberspace superiority surfaces as the outcome of the accelerated time and a digital space-separated singularity that benefit the more-rapid actor. The Zero Domain has a time-space and digital landscape that are accessible only by rapid actors, and a digital landscape that is not accessible by slower actors due to the execution velocity in enhanced accelerated warfare. Velocity achieves cyber Anti-Access/Area Denial (A2/AD), which can be achieved without active initial interchanges by accelerating the execution and cyber ability in a solitaire state. During this process, any adversarial probing engagements only affect the actor on the approach to the Comprehension Barrier; once arrived in the Zero Domain, a complete state of A2/AD is present.

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



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Before joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His website is www.cyberdefense.com.

From that point forward, the actor that reached the Zero Domain has cyberspace singularity and is the only actor who can understand the digital landscape, engage unilaterally without an adversarial ability to counterattack or interfere, and hold the ability to decide when, how, and where to attack. In the Zero Domain, the accelerated singularity controls the battlefield by denying adversarial cyber operations and enacting destruction, extraction, corruption, and exploitation of targeted adversarial digital assets.

Breaking through the comprehension barrier

There is a point along the trajectory of accelerated warfare where only one warfighting nation comprehends what is unfolding and appreciates the cyber terrain. This is the upper barrier for comprehension where the acceleration makes the cyber engagement unilateral. The Comprehension Barrier is dependent on one sides abilities, technical maturity, and institutional structure, and the enemies' weaknesses. Adversaries forged in organizational fear cultures and a strict command structure could, even if technically cognizant and competent, struggle to competitively accelerate the warfare against the more agile and less technically capable opponent. The engagements that accelerate toward the Comprehension Barrier have increased intensity, as they are faster, more forceful, and less restrained when the stress of acceleration degrades the OODA (Observe, Orient, Decide, and Act) loop.

Once the warfighter breaks through the Comprehension Barrier with maintained control, the conflict changes from a contested cyberspace battle to space singularity. The cyber ability in the Zero Domain battle is derived from a single source. At that point, any engagement can affect only the slower party and not the owner of the

Disclaimer: The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the United States Military Academy, or the Department of Defense.

singularity; this is due to the slower attacker's inability to understand the factual battle landscape and target, arrange its resources and conduct warfare at the velocity that occurs on the other side of the Comprehension Barrier. If we use real-life references, the warfighter beyond the Comprehension Barrier has full access to situational awareness, can see the landscape and target, and can act as if the war occurred under normal conditions, while the slower warfighter never reached the Comprehension Barrier is floating weightless in pure darkness. Accelerated warfare beyond the Comprehension Barrier robs the slower party of the ability to understand, sense, order, and coordinate operations. When breaking the Comprehension Barrier, the first of the adversary's final points of comprehension is human deliberation, directly followed by pre-authorization and machine learning, and then these final points of comprehension are passed, and the more-rapid actor enters the Zero Domain.

Time and the lost space

In accelerated cyberwar, time is to cyber what combined time and place were for Clausewitz^[1] because the Zero Domain nullifies the importance of other warfighting domains and creates a parsimonious singularity through the absence of a common battlespace. Space matters only before the Comprehension Barrier is crossed. The traditional concentration of forces—*where* and *when*—is replaced with *then*, because the singularity occurs first in the Zero Domain. As noted strategist Edward N. Luttwak stated, strategies without the ability to execute are pointless exercises.^[2] The accelerated warfare beyond the Comprehension Barrier eradicates the influence of the opponent's cyber strategy because singularity in the Zero Domain removes the opponent's ability to execute.

The evaporated OODA loop

From an operational standpoint, action beyond the Comprehension Barrier evaporates and nullifies the traditional command and control (C2) scheme. In general terms, military C2 follows the steps of the OODA loop developed by U.S. Air Force Colonel John Boyd in the 1960s (Fig. 1).^[3] Accelerated warfare beyond the Comprehension Barrier nullifies the adversary's OODA loop because the rapid-actor leaves the adversary with nothing to accurately observe, no targets to orient toward, no information nor situational awareness with which to make a decision, and the ability to act is limited to spurious actions with no relation to the unfolding events. The unique tenets of cyber undermine the utility of the OODA loop.^[4] The OODA loop requires the ability to assess ongoing events (as in the initial step of "observe"), but under conditions of anonymity, computational speed in cyber execution, and no object permanence, the observations feeding the loop are likely to be inaccurate, if not spurious, as acceleration starts. In accelerated warfare, the OODA loop disappears in the engagement for the slower party if the faster actor breaks the Comprehension Barrier. The rapid-actor maintains its OODA loop in the Zero Domain, and conversely, if the rapid-actor is no longer able to keep its position in the Zero Domain,

the OODA loop will reemerge for the slower actor as the formerly rapid-actor is unable to maintain velocity beyond the Comprehension Barrier.

The “orient” stage in the OODA loop—reacting to unfolding events and positioning for

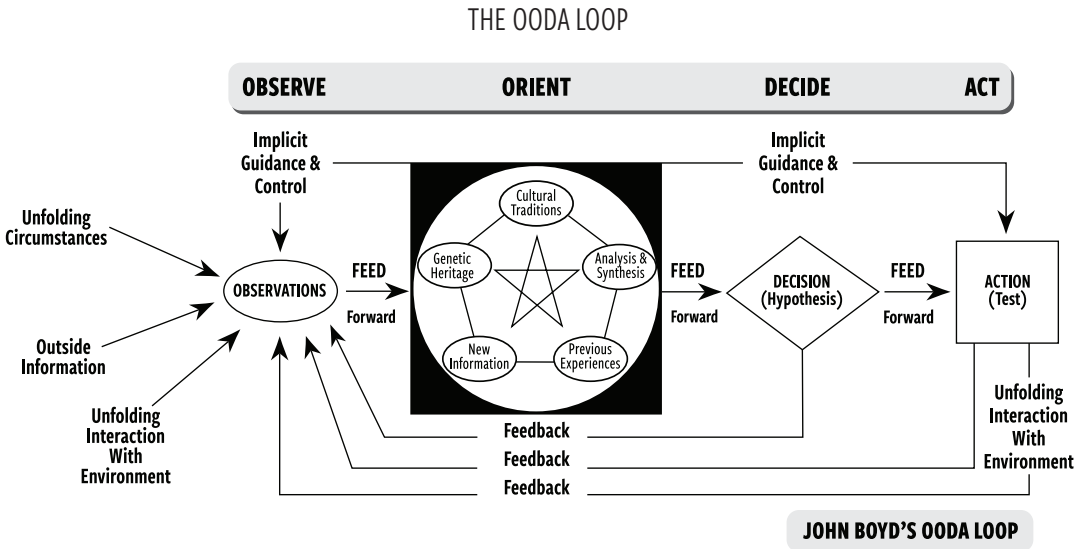


Figure 1. by Patrick Edwin Moran - own work. Licensed under CC BY 3.0 via Wikimedia Commons.

a better outcome—assumes a maneuverable space with favorable positions, but the lack of object permanence in cyber brings an ever-changing battlefield and permanent disorientation rather than re-orientation. When these nodes—ever-changing spaces lacking object permanence—are accelerated beyond the Comprehension Barrier, environmental information cannot be structurally understood or ordered outside of the Zero Domain. If the “observe” and “orient” stages are not relevant to the facts of the engagement, then the “decide” stage will fail to deliver the proper course of action and thus lead to an ineffective “act” stage. Computational speed exacerbates the inability to assess and act, and the increasingly shortened time frames likely to be found in future cyber conflicts will disallow any significant human deliberation. Enemy deliberation, either through leadership or pre-authorization, are ultimately ineffective once the Comprehension Barrier is passed.

The key to victory historically has been the concept of being able to get inside the opponent's OODA loop, and thereby distort, degrade, and derail the opponent's OODA assessments.^[5] In accelerated warfare beyond the Comprehension Barrier, there is no need to be inside the opponent's OODA loop because the accelerated warfare concept removes the OODA loop for the opponent and thereby disabling the opponent's ability to coordinate, seek effect, and command.

The Zero Domain

The five traditional battlespace domains are contested spaces (land, sea, air, space, and cyber) where parties interact, engage, have interchanges through which they can structure their understanding of the battle environment to make decisions. When both parties are present in the engagement, and even if one is weaker and less able to challenge, there is a mutual perception of the framing of the fight. The Zero Domain is the battle space beyond the Comprehension Barrier where battle space singularity occurs, and only one actor has access to the OODA loop. The Zero Domain is the warfighting space where accelerated velocity in the warfighting operations removes the enemy's presence. It is the domain with zero opponents. It is not an area denial, because the enemy is unable to accelerate to the level where it could enter the battle space, and it is not access denial because the enemy is not part of the fight once the Comprehension Barrier is broken. Instead, it is a state of cyber A2/AD, but there is no challenge to this state in the Zero Domain because it is an outfall of the establishment of the Zero Domain.

SHORT CONCLUSION

As a research note, these ideas and concepts are under development and are not the final output. The purpose of the note is to introduce new concepts, open up the discussion, and catalyze comments. ♥

NOTES

1. C. von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.
2. E. Luttwak, *The Grand Strategy of the Roman Empire: From the First Century CE to the Third*. Baltimore, MD: Johns Hopkins University Press, 2016.
3. F. P. B. Osinga, *Science, strategy and war: The strategic theory of John Boyd*. New York, NY: Routledge, 2007.
4. J. Kallberg and T. S. Cook, "The unfitness of traditional military thinking in cyber: Four cyber tenets that undermine traditional strategies," *IEEE Access*, vol. 5, pp. 8126-8130, April 2017. [Online]. Available: ResearchGate, https://www.researchgate.net/publication/317328999_Unfitnessstrationalthinking, accessed August 12, 2018.
5. J. R. Boyd, "The essence of winning and losing," unpublished.

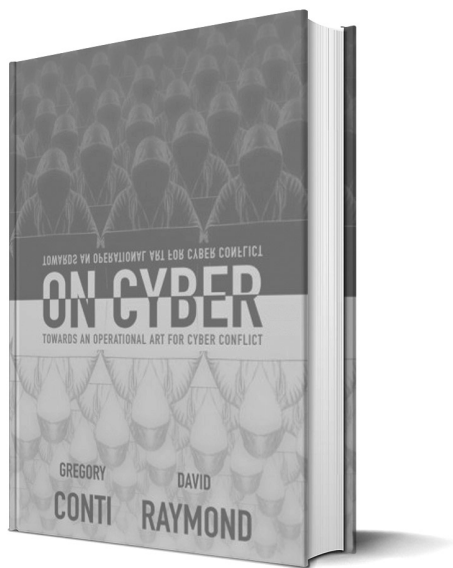
THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆

On Cyber: Towards an Operational Art for Cyber Conflict

by Gregory Conti and David Raymond

Reviewed by
Dr. Jan Kallberg



The core of Conti and Raymond’s *On Cyber: Towards an Operational Art for Cyber Conflict* is found in the preface under the self-explanatory title, “Why this book?” and embedded in the following sentence: “The lack of an operational art for cyberspace operations is the inspiration for this book.” Conti and Raymond have identified a wide and open gap in the cyber literature, found not in the cyber hinterlands, but in the pivotal question of, “how do you do cyber operations?” We are now about 20 years into cyber – 20 years ago, cyber defense and cyber operations were all but unknown, and had less than a few references in the now-defunct AltaVista search engine – and, discussions within the cyber community still occur mainly at the strategic and conceptual level, or at the purely tactical level. The larger policy debate is driven by a non-technical community, and the tactical level quickly becomes highly technical as a subset of computer science.

This is where Conti and Raymond’s *On Cyber* found the key terrain and gap in the literature. Both Conti and Raymond are retired Army officers with a background in cyber, and former ACI colleagues. The title, *On Cyber*, resembles Carl von Clausewitz’s classic *On War*, a bold move that raises reader expectations. Conti and Raymond do not claim that their work is the end state of the discipline, or that they have figured it out, but instead invite the cyber community to take a leap forward with them to catalyze activity in the community. Conti and Raymond are eager to force us to think about cyber in an operational context, and stoke our intellectual fire to drive the discourse forward.

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



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

They succeed because, whether it was done on purpose or not, one cannot merely read the book and silently take in the words. Instead, the reader will think, assess, evaluate, agree, disagree, reject, and accept, all of which is beneficial.

Some factors are normally less frequent in cyber works, but are central to cyber as an environment, such as speed and intensity of engagement, and perception of presence in an environment with no object permanence. Conti and Raymond cover these topics and show a clear and well-founded understanding of the unique cyber landscape.

Conti and Raymond also devote significant time and space explaining why things are the way they are, and seek to explain terms, definitions, and arrangements with high granularity and precision. After reading the book, one realizes that this intellectual calibration is a well-thought-out tool to help the reader. The information security community has used military terms loosely in recent decades to explain actions and activities, while the marketing of cybersecurity products and services has diluted the power of the terminology as it fits with marketing plans. The cyber community frequently employs powerful words that lack a common understanding. Military terminology's sole purpose is to communicate with clarity regarding the expectations, activities, and resources required. Once one knows the terminology, the book opens up as a cryptographic key. The inherent power of well-understood terms became apparent to me in my second reading of the book.

The thread woven through Conti and Raymond's *On Cyber* is educational, supported by almost 700 references, with an invitation to challenge their approaches. The book is true to cyber, and that is what makes it worth reading and returning to for inspiration and guidance. 🛡️

Title: *On Cyber: Towards an Operational Art for Cyber Conflict*

Author: Gregory Conti and David Raymond

Publisher: Kopidion Press; first edition
(July 17, 2017)

Hardcover: 108 pages

Language: English

ISBN-10: 0692911561

ISBN-13: 978-0692911563

Price: \$35.00

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

 cyberdefensereview.army.mil

AND THROUGH SOCIAL MEDIA

 Facebook [@army cyber institute](https://www.facebook.com/army cyber institute)

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



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.