

# THE CYBER DEFENSE REVIEW



*A Conversation with  
General (Ret.) David H. Petraeus*



How Could They Not: Thinking Like  
a State Cyber Threat Actor

*Dr. Gregory Conti  
Dr. Robert Fanelli*

Artificial Intelligence in Digital Warfare:  
Introducing the Concept  
of the Cyberteammate

*Dr. Rudy Guyonneau  
Arnaud Le Dez*

The Post-GIG Era: From Network  
Security to Mission Assurance

*Dr. Kamal Jabbour*

A Case for Action: Changing the  
Focus of National Cyber Defense

*Rob Schrier*

Data Privacy and Protection:  
What Businesses Should Do

*Kiersten E. Todt*

---

## INTRODUCTION

*The Cyber Defense Review:*  
Defending Forward

*Colonel Andrew O. Hall*

## BOOK REVIEW

*Dawn of the Code War*  
by John P. Carlin

*Philip C. Shackelford*



# 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. Mark Visger, J.D.  
(Cyber Law)

### EDITORIAL BOARD

Col. Andrew O. Hall, Ph.D. (Chair.)  
U.S. Military Academy

Dr. Amy Apon  
Clemson University

Dr. Chris Arney  
U.S. Military Academy

Dr. David Brumley  
Carnegie Mellon University

Dr. Martin Libicki  
U.S. Naval Academy

Ms. Merle Maigre  
CybExer Technologies

Dr. Michele L. Malvesti  
Financial Integrity Network

Dr. Milton Mueller  
Georgia Tech School of Public Policy

Dr. Hy S. Rothstein  
Naval Postgraduate School

Dr. Bhavani Thuraisingham  
The University of Texas at Dallas

Ms. Liis Vihul  
Cyber Law International

Prof. Tim Watson  
University of Warwick, UK

### CREATIVE DIRECTORS

Sergio Analco  
Gina Daschbach

### LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

### PUBLIC AFFAIRS OFFICER

Capt. Lisa Beum

### KEY CONTRIBUTORS

Clare Blackmon  
Nataliya Brantly

Kate Brown  
Erik Dean

Shane Fonyi  
Col. John Giordano

Lance Latimer  
Eric Luke

Alfred Pacenza  
Diane Peluso

Irina Garrido de Stanton  
Michelle Marie Wallace

### CONTACT

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

### SUBMISSIONS

The Cyber Defense Review  
welcomes submissions at  
[mc04.manuscriptcentral.com/cyberdr](https://mc04.manuscriptcentral.com/cyberdr)

### WEBSITE

[cyberdefensereview.army.mil](https://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. The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.*

---

---

INTRODUCTION

<b>COLONEL ANDREW O. HALL</b>	9	<i>The Cyber Defense Review: Defending Forward</i>
-------------------------------	---	--

---

SENIOR LEADER INTERVIEW

<b>A CONVERSATION WITH GENERAL (RET.) DAVID H. PETRAEUS</b>	15	
---	----	--

---

SENIOR LEADER PERSPECTIVE

<b>ROB SCHRIER</b>	23	A Case for Action: Changing the Focus of National Cyber Defense
--------------------	----	--

---

PROFESSIONAL COMMENTARY

<b>MAJOR NATHANIEL D. BASTIAN, PH.D.</b>	31	Information Warfare and Its 18 <sup>th</sup> and 19 <sup>th</sup> Century Roots
<b>KIERSTEN E. TODT</b>	39	Data Privacy and Protection: What Businesses Should Do

---

RESEARCH ARTICLES

<b>DR. GREGORY CONTI DR. ROBERT FANELLI</b>	49	How Could They Not: Thinking Like a State Cyber Threat Actor
---	----	---

<b>HALLIE COYNE</b>	65	The Untold Story of Edward Snowden's Impact on the GDPR
---------------------	----	--

<b>MAJOR (RET.) JACOB COX, PH.D. COLONEL DANIEL BENNETT, PH.D. COLONEL (RET.) SCOTT LATHROP, PH.D. LIEUTENANT COLONEL (RET.) CHRIS WALLS CHIEF WARRANT OFFICER 4 (RET.) JASON LACLAIR LIEUTENANT COLONEL CLINT TRACY CHIEF WARRANT OFFICER 4 JUDY ESQUIBEL</b>	81	The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence
--	----	---

## RESEARCH ARTICLES

**DR. RUDY GUYONNEAU**  
**ARNAUD LE DEZ**

103

Artificial Intelligence in Digital Warfare:  
Introducing the Concept of the  
Cyberteammate

**DR. KAMAL JABBOUR, ST**

117

The Post-GIG Era: From Network  
Security to Mission Assurance

---

## RESEARCH NOTE

**LIEUTENANT COLONEL**  
**DAVID M. BESKOW**  
**DR. KATHLEEN M. CARLEY**

131

Future Geospatial Disinformation  
Campaigns

---

## BOOK REVIEW

**PHILIP C. SHACKELFORD**

141

*Dawn of the Code War*  
by John P. Carlin





# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆



VOLUME 4 ♦ NUMBER 2

## *The Cyber Defense Review:* Defending Forward

Colonel Andrew O. Hall



### INTRODUCTION

Welcome to the Fall edition of *The Cyber Defense Review* (CDR). This tenth edition of the CDR is published in conjunction with the Army Cyber Institute's (ACI) International Conference on Cyber Conflict U.S. (CyCon U.S.), which takes place November 18-20, at the Crystal Gateway Marriott in Arlington, VA. The CyCon U.S. conference is the premier forum on cyber conflict. Just like the CDR, the CyCon U.S. conference provides a venue for fresh ideas, relevant and actionable content, insight into future trends, and access to industry, government, and military leaders, cyber innovators, and pioneers in the discipline. The conference promotes multidisciplinary cyber initiatives and furthers research and cooperation on cyber threats and opportunities. The CyCon U.S. conference is a collaborative effort between the ACI at West Point and the NATO Cooperative Cyber Defence Centre of Excellence and complements the CyCon Conference held every May in Estonia.

This year's CyCon U.S. theme is Defending Forward, which is also the Department of Defense's (DoD) 2018 Cyber Strategy. Defending Forward identifies the need for active preparedness in cyberspace by disrupting or halting malicious cyber activity at its source and degrading said activity before it can reach its intended victim. This preemptive strategy advocates defending resources, from military operations to financial institutions, in both the public and private sectors. Critical infrastructure and sectors of the economy that are considered vital to the nation's economic prosperity are consistently scrutinized and exploited by several well-known cyber tools and techniques.

We are excited to publish the CyCon U.S. conference papers in the Winter 2020 CDR. This Special Edition of the CDR will feature five technical and seven policy papers that dramatically provide texture and insight into the complicated Defending Forward strategy. Also, the CDR continues a proud relationship with JSTOR's Security Studies collection.

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



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

This edition of the CDR carries the message of Defending Forward and is our most robust, diverse, and thought-provoking. The Fall CDR includes an exclusive leadership interview, leadership and professional commentaries, research articles, a research note, and our featured book review. We are honored to have the opportunity to interview GEN (Ret.) David Petraeus for this edition. He is a warrior and scholar and one of this country's premier strategic thinkers. This interview will be a must-read for all cyber leaders and practitioners. GEN Petraeus fielded relevant questions from a team of ACI research scientists on the viability of comprehensive security.

The Fall CDR features a leadership perspective article from Mr. Robert Schrier, the Chief of Staff of Asymmetric Operations Sector of Johns Hopkins Applied Physics Laboratory. Mr. Schrier is retired from DoD Senior Executive Service where he last served as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. In his powerful work "Case for Action - Changing the Focus of National Cyber Defense," Mr. Schrier challenges the nation to create processes and capabilities to prevent, deter, and preempt cyber-attacks against our critical infrastructure, as well as to interdict and counter those attacks.

Our Professional Commentary section begins with the article "Information Warfare and its 18th and 19th Century Roots" by MAJ Nathaniel Bastian, Ph.D. He is formerly of the ACI and now working as a Senior Data Scientist and AI Specialist within the Capability Delivery Directorate of the Joint Artificial Intelligence Center (JAIC). This critical commentary takes a penetrating look into the historical implications impacting today's Information Warfare landscape. Continuing with our Professional Commentaries, we have an excellent article by Kiersten E. Todt, Resident Scholar at the University of Pittsburg's Institute for Cyber Law, Policy, and Security. In "Data Privacy and Protection: What Businesses Should Do," Ms. Todt gives readers three specific

mechanisms that companies should employ to ensure the privacy and protection of their customers and clients.

Our CDR readers will thoroughly enjoy all five scholarly research articles. Dr. Kamal Jabour, Air Force Senior Scientist for Information Assurance presents CDR readers with a paradigm shift from cybersecurity through network defense to mission assurance through information assurance. Dr. Greg Conti and Dr. Bob Fanelli from IronNet Cybersecurity presents a valuable study that explores the profound cyber threat from State actors. Ms. Hallie Coyne takes an exhaustive look at Edward Snowden and the origins of the General Data Protection Regulation (GDPR). The CDR showcases the work of Dr. Jacob Cox, COL Daniel Bennett, Ph.D., COL (Ret.) Scott Lathrop, Ph.D., LTC (Ret.) Christopher Walls, CW4 (Ret.) Jason LaClair, LTC Clint Tracy, and CW4 Judy Esquibel with their study of electronic warfare and cyber convergence. We feature two brilliant French cyber scholars, Dr. Rudy Guyonneau from Sopra Steria SA and LTC Arnaud Le Dez from Saint-Cyr Military Academy as they provide a breathtaking look at Artificial Intelligence and the future of cyber warfare.

The CDR continues with its high-velocity research note section with an exciting article from LTC David Beskow and Dr. Kathleen Carley, both from Carnegie Mellon University as they investigate geospatial disinformation campaigns. If you are looking for an exceptional cyber read, Mr. Philip Shackelford's review of "Dawn of the Code War" by John P. Carlin, sheds light on the cyber struggles the U.S. Government faces each day.

I'm delighted to announce the ACI's publication of *Nonsimplicity, The Warrior's Way* by Dr. Bruce West and Dr. Chris Arney. This essential scholarly work addresses what complexity science suggests are the appropriate changes and implications in policies, procedures, and principles for the individual within the military. We are also excited to announce that the CDR's Digital Editor is currently working on a more up-to-date and academic website that will continue to push the cyber conversation. I encourage our readers to submit research papers, commentaries, research notes, book reviews, or blogs on the CDR *ScholarOne* platform: <https://mc04.manuscriptcentral.com/cyberdr>.

Please check our Call for Papers announcement on the CDR website to submit articles on "Information Operations" for a themed Summer 2020 CDR: <https://cyberdefensereview.army.mil/>. Information Operations is critical to military leaders and policymakers as they develop strategies to support the nation. We welcome a multidisciplinary and international examination of this important topic.

I want to recognize the remarkable talent and creativity of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, SGM Jeff Morris, Courtney Gordon-Tennant, and the special members of the West Point Class of '70 in shaping this important edition. As always, we are excited to continue the cyber conversation together!💙



# THE CYBER DEFENSE REVIEW

◆ INTERVIEW ◆





# A Conversation with General (Ret.) David H. Petraeus

---

Cyber operations are a perfect example of how efforts in one domain can affect virtually every aspect of a nation's comprehensive security. The CDR was keenly interested in General David Petraeus' view of comprehensive security, its whole-of-government implications, and its critical importance to the United States. The interview was conducted via email during April and September of 2019.

**The Cyber Defense Review (CDR):** The 2018 DoD Cyber Strategy and GEN Paul Nakasone's February 2019 Congressional testimony describe a new, emerging strategic environment in cyberspace characterized by "great power competition" or "strategic competition" with China, Russia, and others. The dynamics of this new environment are perhaps most salient in cyberspace, with the US confronting near-peer and arguably even peer competitors, and where, due to the reliance of our economy and society on IT-connected infrastructure, the US is particularly vulnerable. This strategic competition extends well beyond cyberspace, to include political, military, and economic competitions across all other domains and instruments of power. How do you see strategic competition in cyberspace in relation to the other domains of warfare?

**General (Ret.) David H. Petraeus:** *Cyberspace is the newest domain of warfare, and is now very much front and center, joining land, air, sea, and space. It is also the domain in which "warfare" is already ongoing on a daily basis, as state and non-state actors probe our cyber defenses, conduct cyber reconnaissance of critical infrastructure control systems, try to inspire and direct extremist activities, seek to steal secrets and intellectual property, attempt to influence our debates and elections, and carry out criminal acts, among many other activities. Beyond that, any future military campaign inevitably will entail increasingly complex and important offensive and defensive cyberspace operations that complement operations in other domains, employing cyberspace capabilities to help defend our systems and also to degrade, disrupt, and defeat our adversaries' systems and networks that depend on cyber connectivity and other aspects of cyberspace.*

© 2019 General (Ret.) David H. Petraeus



**General David H. Petraeus (U.S. Army, Ret.)** is a Partner with the global investment firm KKR and Chairman of the KKR Global Institute. He also serves on the boards of two KKR-owned companies, Optiv (a major cybersecurity firm) and OneStream (a leading business software provider), as well as the boards of a number of think tanks and numerous veterans service organizations. Additionally, he is a private venture capitalist with investments in well over a dozen startups. He previously served over 37 years in uniform and then was Director of the CIA. He culminated his military career with six consecutive commands, five in combat, including Command of the Multinational Force-Iraq during the “Surge,” US Central Command, and the International Security Assistance Force in Afghanistan. A graduate, with distinction, from the U.S. Military Academy in 1974, General Petraeus later earned a Ph.D. from Princeton University in a multi-disciplinary program in international relations and economics. General Petraeus has held academic appointments at the U.S. Military Academy, the City University of New York’s Honors College, the University of Southern California, and Harvard’s Belfer Center. His numerous awards and decorations include four Defense Distinguished Service Medals, the Bronze Star Medal for Valor, the Combat Action Badge, the Ranger Tab, and Master Parachutist Wings. He has also been decorated by 13 foreign countries.

**CDR:** Your career has provided you with the unique opportunity to have an impact at senior levels in both the government and the private sector. Our adversaries carry out sophisticated cyber campaigns targeting the private sector; and the DoD has a mandate to “defend the Nation” in cyberspace, which includes the economic engines in the private sector. Given your experience, how can the U.S. Government and our private sector better collaborate to defend the Nation in cyberspace?

**GEN (Ret.) Petraeus:** *In recent years, the U.S. Government has taken many actions to improve our Nation’s defenses (and offensive capabilities) in cyberspace, though clearly more work is required.*

*Elevating U.S. Cyber Command (USCYBERCOM) to a fully-fledged combatant command in May 2018 was one (overdue) such action; and much more work needs to be done to fully define roles and missions of USCYBERCOM overall and the National Security Agency (NSA) and USCYBERCOM’s other components individually, as well as its ultimate organizational architecture. Among these, the Department of Defense (DoD) still needs to resolve whether USCYBERCOM is, in essence, a military service (that recruits, trains, educates, equips, develops, etc.), a geographic combatant command (with cyberspace as its area of responsibility), or a functional combatant command (such as U.S. Special Operations Command)—or will perform tasks of all three, which I support, but which will also require in-depth conceptual work, as this in many respects would present a new paradigm for our military.*

*The establishment of the Cybersecurity and Critical Infrastructure Security Agency (CISA) within the Department of Homeland Security last fall was another positive step, one that many of us argued for some time ago. Nonetheless, much hard work is needed to build CISA concepts and capabilities, to recruit needed personnel, to enact enabling legislation, to build up required resources, and to implement the policies and regulations that will optimize our ability to operate in this newest warfare domain.*

*Finally, the establishment four years ago of the Cyber Threat Intelligence Integration Center in the Director of National Intelligence headquarters was another critical step, given that intelligence on state and non-state actors in cyberspace is so important to government cybersecurity activities, but also, through various methods of sharing, for private-sector cybersecurity firms and US companies, as well.*

*Needless to say, government efforts are complemented in a very significant manner by a growing number of cybersecurity firms, products, capabilities, and integrators. And there is healthy collaboration among them, the intelligence community, U.S. executive departments that operate in this arena, and various national (especially the FBI as the lead federal agency for cybercrime investigation), state, and local law enforcement agencies.*

*Despite these actions and a number of others, I suspect that most individuals engaged in either government or private sector cybersecurity would acknowledge that the challenges continue to get ever more complex and sophisticated—and that it is hard just to keep pace with them conceptually, much less get the new legislation, resources, organizations, capabilities, policies, and regulations needed to cope with the evolving challenges in a timely manner. It would be accurate, I think, to observe that we need substantially to “pick up the pace” in this public-private partnership arena if we are to effectively counter the cyber threats we currently face, and which will inevitably grow in scope and complexity. (The NSA’s newly announced Cybersecurity Directorate likely will help in this area.)*

**CDR:** As the global strategic environment evolves in complexity, volatility, uncertainty, and ambiguity, it is critically important to analyze how the Army’s talent management strategy recruits Soldiers for service in the future strategic cyber environment. What strategy should the Army install to attract cyber talent?

**GEN (Ret.) Petraeus:** *I think the Army has a reasonable sense of what is required to attract great cyber talent. That said, it needs to work very hard at this task. Being a cyber warrior clearly provides the extraordinary privilege of performing tasks that protect our country and way of life. That special privilege that will animate many. But recruiting great talent will also require special incentives in terms of compensation, fully-funded and cutting-edge training and education, opportunities with industry, and so forth. Of course, at the end of the day, there is always the intriguing reality that military cyber warriors can take actions in cyberspace that are not permissible in the private sector.*

*Retention is another big challenge, of course, and one must recognize that even special compensation in uniform is unlikely to compete with Silicon Valley salaries; nonetheless, the opportunity, again, to perform missions larger than self together with others who also appreciate that opportunity, is very special. And, combining that motivation and the incentives I mention above has enabled NSA and the newer service cyber organizations to demonstrate an impressive ability to recruit and retain high quality cyber experts. Undoubtedly, though, recruiting and retention in this space will continue to be challenging.*

**CDR:** The Russian and US information warfare capabilities seems to be growing at an alarming rate. Russians have successfully operationalized the Gerasimov Doctrine in Crimea and Ukraine, using information in conjunction with intelligence and special forces operations to achieve some strategic outcomes at relatively low cost. Likewise, as the DNI Report (January 6, 2017) confirmed, Russians manipulated social media platforms such as Facebook and Twitter during the 2016 US Presidential election. There is evidence that Russians also interfered in the UK's Brexit referendum. Despite Russian success in information warfare the Pentagon continues to think conventionally, such as hardening conventional forces in Poland to deter Putin. In your opinion, how does the US correct its course to compete in the information space?

**GEN (Ret.) Petraeus:** *The press in recent years has reported integration of U.S. military cyberspace operations with other warfare domain operations in ongoing campaigns against Islamist extremist organizations.*

*For example, starting over three years ago, Task Force Ares activities complemented Coalition Joint Task Force actions on land and in the air, as well as our host nation partner's actions on the frontlines in Iraq and Syria that ultimately defeated the Islamic State in those countries (though disturbing remnants of IS remain). More recently, USCYBERCOM reportedly has exploited new authorities by taking offensive actions against foreign entities seeking to undermine democracy in the US, to include Russian entities seeking to interfere in the 2018 mid-term elections. The Department of Justice has pursued legal action in several cases against state and non-state actors, as well. And various diplomatic initiatives have also been pursued, including President Obama's pushback against China's theft of US intellectual property.*

*Those actions have been steps in the right direction. But it is clear that more needs to be done, employing every tool available to the US, our Government, and private sector, and that all government and private sector elements must collaborate better and accomplish more.*

**CDR:** The DoD 2018 Cyber Strategy has adopted a more aggressive strategy of countering our adversaries in cyberspace with a policy of "Defend Forward," with an expanded focus of preventing and responding to cyberattacks that are below the threshold of military use of force. More recently, news reports have circulated that USCYBERCOM has engaged in its first such operation, taking offline a so-called Russian "troll farm" on election day in November 2018. Do you see this new development as an appropriate domain for the military since such operations will occur below the use of force threshold, and will likely be in defense of private entities and infrastructure?

## A CONVERSATION WITH GENERAL (RET.) DAVID H. PETRAEUS

*GEN (Ret.) Petraeus: I very much see it that way, and I strongly support the recent authorizations given to USCYBERCOM. But, as I noted in answering the previous question, I think the US will need to employ more aggressively all the capabilities available to us—legal, financial, diplomatic, cyber, and, in some cases, even military. As is often the case, a comprehensive, integrated approach is required. And inevitably, that will require overall coordination by the White House and executive branch departments and agencies, as has been seen in the current and past administrations, in particular. Going forward, in the years ahead, this coordination must be robustly resourced and maintained as one of our Nation's top priorities. 🛡️*



GEN (Ret.) David Petraeus with West Point Cadets at the 2018 International Conference on Cyber Conflict in Tallinn, Estonia.



# THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆





# A Case for Action: Changing the Focus of National Cyber Defense

---

Rob Schrier

**T**he United States government has made major strides in the past year in improving our nation's cyber defense with initiatives such as the creation of the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the new DoD Defend Forward policies. However, our nation's emphasis remains focused on improving collaboration and synchronization primarily to improve reaction and response to a cyber incidents and attacks. We must change the goal to move our emphasis to the "left of boom," to create processes and capabilities to prevent, deter and preempt cyber-attacks against our critical infrastructure, as well as interdict and counter those attacks as they are unfolding. We need to regard response as our last resort. We must create a transformative effort to focus speed, agility, unity of purpose, and early warning and to fully incorporate private industry and other partners. Equally important, we cannot revolutionize cyber defense without including an emphasis on defending our democracy, our society and the truth itself from cyber driven influence attacks. I propose the creation of a national level 24/7 cyber defense operational capability with an initial pilot operation focused on defending our democracy in the U.S 2020 elections.

So is our original goal possible? Can we move our cyber defense largely "left of boom"? Can we defend against influence attacks? Can all this be practically achieved? Yes, we can decide to dramatically improve the defense of our critical infrastructure and defend our democracy within our existing laws and policies in a more preemptive and effective manner. We must feel a sense of urgency to accomplish this. This is not a philosophical discussion based on the assumption that the wolves could reach our gates. Because we have ceded our adversaries too much access, the wolves are already inside our gates. Our adversaries have been, are now, and will be conducting increasingly bold and sophisticated attacks against US critical infrastructure and our democracy. We have every reason to expect these cyber and influence attacks will grow more serious. The increasing risks to democracy and, more broadly, to our way of life are too worrisome to ignore.



**Mr. Rob Schrier** is currently the Chief of Staff of Asymmetric Operations Sector of Johns Hopkins Applied Physics Laboratory. He leads research on military cyber and Information Operations. He moved to the Laboratory after retiring from the DoD Senior Executive Service after a thirty-six year career. He served as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. Mr. Schrier was a plank holder on the team who established U.S. Cyber Command and served as the initial Deputy Director for Current Operations. Throughout his career, he held a variety of DoD leadership positions after beginning his career as an analyst. Mr. Schrier has more than ten years' experience as a leader in cyber operations. Mr. Schrier earned a Bachelor of Arts Degree from the University of Maryland, a Master of Science Degree in Applied Behavioral Science from Johns Hopkins University and attended the Chairman, Joint Chiefs of Staff CAPSTONE Course.

We need to create a national level 24/7 cyber defense operational capability to change this paradigm with the creation of the National Cyber Operational Defense Cell (NCODC). Names matter. This activity is national in nature. It is cyber in nature (which incorporates influence). It is bound by operational activity and focused on defense. Finally, the word “cell” denotes that this is a lean rather than monolithic function. The NCODC will give us the speed, agility, unity of purpose, and operational connection with private industry and other partners that will change the current paradigm with our adversaries and allow us to gain an upper hand. The NCODC can successfully work on a practical level. So, let’s start with what the NCODC will do:

- ◆ Direct and synchronize operations to prevent, deter, preempt, interdict and counter adversary activity through a 24/7 operations center that will include operational level participation by key U.S. Government players as well as “authorized to act” Critical Infrastructure private industry representatives. This organization will be operationally focused on defensive actions including executing defend forward actions. This is not an organization designed to expand into a policy organization or replace other functions in the individual government agencies or the military. The sole goal of this cell is to achieve speed, agility, and unity of effort in defending our nation against cyber-attacks and trying to move the bulk of that defense “left of boom.” Individual government elements (such as U.S. Cyber Command and FBI) would bring their authorities and execute their own operations but under the timing and tempo directed by the NCODC Director. There will be thresholds to establish what level of operation fits into this process.

- ◆ Drive improvements in both actionable early warning and near real-time intelligence to drive our cyber operations. Utilize publicly available cyber data in addition to classified intelligence to provide the early warning needed to enable our forces to prevent, deter, preempt, interdict, and counter cyber and cyber driven influence attacks.
- ◆ Lead the cyber interagency and foreign partner process for imminent and ongoing operations.

**There are reasons why creating this new cyber defense function will be daunting:**

- ◆ The NCODC may initially be unpalatable to stakeholders in government and military cyber organizations and these cyber organizations may initially be against the concept.
- ◆ The U.S. Government is historically inefficient at creating new organizations.
- ◆ The private sector may see the NCODC as both government mission creep into private sector business and a further risk to our civil liberties.
- ◆ There is no real US precedent for a continuous 24/7 national level operational activity of this nature.
- ◆ Most Americans still do not recognize the seriousness of the cyber and influence threat to our nation.
- ◆ There may be a perception this will be a high cost.
- ◆ This will take a high degree of non-partisan political will not prevalent today.

**Why this could fail:**

- ◆ Partisan politics may not allow the idea to gain traction.
- ◆ The new organization may not survive political infighting by the contributing organizations.
- ◆ The selected NCODC leadership may not be bi-partisan or apolitical.
- ◆ The private sector may decide against active participation.
- ◆ Most likely, there will be enough political will to create the function in a limited fashion, but the compromises agreed to during its mission formulation may dilute it from a 24/7 operational activity to yet another collaborative body where each contributing element continues to act independently, thereby defeating the original goal of speed, agility, and unity of purpose.
- ◆ The NCODC will weaken into a synchronization and not exist as an operational cell.

**How we can succeed:**

- ◆ We will achieve efficiency and save most of the cost by not creating a new organization from zero.

- ◆ We will name a leadership team and small stand-up strategy team with operational DoD, FBI, DHS and IC participation. We will have the top NCODC leadership focused on operations. These leaders must be perceived by all as nonpartisan and apolitical.
  - The Director will be a political appointee who has real experience in military cyber, government cyber, and in the private industry, but has remained apolitical.
  - The Commander of U.S. Cyber Command Cyber National Mission Force (CNMF) serves as the Deputy Director in a dual-hatted role.
  - The DHS NCICC Director will also serve as the Executive Director a dual-hatted role.
  - An FBI Cyber leader will also serve as the Director of Intelligence in a dual-hatted role.
  - A special Counter-Intelligence leadership role will be created for a CIA representative.
  - Create an industry advisory group (authorized to act) who is fully cleared to work in the Operations Center. This will be the difference maker and will take additional thought beyond this article.
  - Do not create a new, costly operations floor. Initially house this new effort either in existing DHS or U.S. Cyber Command Joint Operations Center spaces.
  - Start with modest funding and increase funding annually.
  - Using a structure akin to a J-Code structure should create staffing efficiency and effectiveness.
  - Most importantly, initiate this new function starting with the 2020 elections pilot activity.

***NCODC Pilot Activity: Defending the 2020 Elections***

- ◆ Create a pilot activity beginning in Fall 2019 to lead the coordinated cyber defense of our 2020 Presidential and Congressional elections across the cyber influence spectrum. This will be an initial, specific, bound activity where speed, agility, and unity of effort will be crucial to our success. The pilot operation will give us the best opportunity to change our focus from responding after attacks to preventing, deterring, and preempting, interdicting, and countering cyber-influence attacks against our democratic processes. Our adversaries will undoubtedly have increased their aggressive intent for the 2020 elections, and we want to be postured to meet them as far “left of boom” as possible. We should stand the initial pilot activity up immediately and build the full NCODC as I prescribed.♥

***Personal Qualifier*** – These thoughts were written by Robert A. Schrier, retired DoD SES, on a voluntary basis as a retired DoD employee. These are his personal views and do not reflect the views of the DoD, the USG or his current employer, Johns Hopkins Applied Physics Laboratory.





# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆





# Information Warfare and Its 18<sup>th</sup> and 19<sup>th</sup> Century Roots

---

Major Nathaniel D. Bastian, Ph.D.

For Joint Force leaders to visualize and describe how the operational environment shapes the range of military operations, they must have a deep understanding of the capabilities comprising the multi-domain battlefield. The information environment, which Joint Publication (JP) 3-13 defines as the “aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information,”<sup>[1]</sup> is intrinsically linked to the traditional land, air, maritime and space domains. Moreover, the rapid advancement and application of technologies has directly facilitated the use of information-related capabilities in Joint Force operations.<sup>[2]</sup> The orchestrated use of these information activities, commonly known as “information operations”, aims to gain strategic and operational advantages in the information environment.<sup>[3]</sup> These advantages are often gained through the manipulation of the information environment using information operations (IO), which, according to JP 3-13, are the “integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.”<sup>[4]</sup>

Some historians hold that information warfare dates from the beginning of the 20<sup>th</sup> century, noting, for example, that the French army conducted IO activities in the First World War, using electronic warfare techniques that enabled the interception of wireless and telephone communications.<sup>[5]</sup> Yet, history confirms otherwise - appreciation for the value of intelligence dates to Sun Tzu and earlier, and 18<sup>th</sup> and 19<sup>th</sup> century leaders conducted information warfare using information-related intelligence gathering, military deception, military information support operations, and operations security. Examining these roots of modern-day information operations can yield valuable insights.

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



**MAJ Nathaniel D. Bastian, Ph.D.** serves as Senior Data Scientist and Artificial Intelligence (AI) Engineer at the Department of Defense (DoD) Joint Artificial Intelligence Center. He provides technical advisement for AI research, design conceptualization, prototyping, systems architecture, product development, and software deployment, leading to the operationalization of AI-enabled products and technologies to solve novel, complex problems that span the DoD. MAJ Bastian previously served as Operations Research Scientist and Assistant Professor at the Army Cyber Institute at the U.S. Military Academy, where he led cyber research efforts within the Intelligent Cyber-Systems and Analytics Research Laboratory. He holds a Ph.D. degree in Industrial Engineering and Operations Research from the Pennsylvania State University, M.Eng. degree in Industrial Engineering from Penn State, M.S. degree in Econometrics and Operations Research from Maastricht University, and B.S. degree in Engineering Management (electrical engineering) with honors from the U.S. Military Academy at West Point.

A multitude of military capabilities contribute to information warfare. Intelligence gathering is a primary tool for assessing the information environment because it significantly enhances Joint Force leaders' understanding of the relationships among the physical, informational, and cognitive dimensions.<sup>[6]</sup> The primary purpose of information collection, analysis, and dissemination has not changed, but intelligence gathering has evolved since the 18<sup>th</sup> century.<sup>[7]</sup> In the mid-1750s, for example, Frederick the Great employed a most impressive long-term intelligence system for gathering information.<sup>[8]</sup> In fact, according to Christopher Duffy, Frederick pumped “travelers for news of the tactics and weapons of his potential enemies, and, indeed, for any information that might enable him to build up character-pictures of their rulers and generals.”<sup>[9]</sup> Moreover, he created spy networks by planting Prussian agents in enemy countries to establish information channels, and Duffy contends that he briefed his Prussian officers to conduct reconnaissance on roads, passes, rivers, bridges and other terrain when traveling.<sup>[10]</sup> Similar to today, Frederick’s primary reason for using intelligence gathering on the battlefield was to learn about an adversary or enemy’s potential capabilities or vulnerabilities.<sup>[11]</sup> Despite his extensive use of intelligence gathering, however, Frederick was often challenged in his efforts to obtain reliable, accurate information about enemy battle plans.<sup>[12]</sup>

This challenge was underscored by Carl von Clausewitz, who observed that “many intelligence reports in war are contradictory; even more are false, and most are uncertain [...] the reports turn out to be lies, exaggerations, errors, and so on. In short, most intelligence is false, and the effect of fear is to multiply lies and inaccuracies.”<sup>[13]</sup> Despite these inherent imperfections associated with intelligence gathering, its use as an integral component of information warfare is not a modern-day concept. As noted, Frederick the Great conducted information warfare using intelligence gathering because he wanted to leverage the information

collected for operational and tactical planning, as well as determine the most effective way to elicit the specific response he desired from the enemy or adversary.<sup>[14]</sup>

In addition to intelligence gathering, 18<sup>th</sup> century leaders targeted information warfare against enemy decision-making processes. Military deception (MILDEC) is one such information-related capability that these leaders used. They would attempt to influence an adversary's perceptions via actions that they executed deliberately to mislead adversary decision makers.<sup>[15]</sup> Duffy reports that Frederick the Great thoroughly relished using tricks and ruses to conceal his own intentions; he had roads repaired as if in preparation for a retreat, assigned fictional names to regiments, and even arranged the capture of his couriers who had false messages.<sup>[16]</sup> As evidenced, Frederick the Great employed MILDEC to lead adversary military decision makers to incorrect conclusions about his force's capabilities and intentions by targeting their informational and cognitive processes.<sup>[17]</sup> Unlike Frederick the Great, however, Clausewitz viewed MILDEC as mostly ineffective as the general officer qualities of deception (craft, cleverness, and cunning) were not prominent in the history of war.<sup>[18]</sup> Clausewitz saw limited value in the issuance of false plans, orders and reports to sow confusion in the enemy.<sup>[19]</sup> Despite Clausewitz's general negative view of MILDEC, he did proffer that "when prudence, judgment, and ability no longer suffice, cunning may well appear the only hope."<sup>[20]</sup> While Frederick the Great and Clausewitz seem to have disagreed on the effectiveness of using MILDEC, history confirms that 18<sup>th</sup> century leaders did conduct information warfare by employing IO activities, particularly deception. This resonates with Sun Tzu's perspective that warfare is based upon deception.<sup>[21]</sup>

Not only did 18<sup>th</sup> century leaders employ MILDEC as an information-related capability; 19<sup>th</sup> century leaders also conducted information warfare via military information support operations (MISO). JP 3-13.2 defines MISO as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."<sup>[22]</sup> For example, Michael Hughes suggests that Napoleon often issued proclamations to portray France as the victim of foreign aggression while serving as the French Emperor in the early 1800s.<sup>[23]</sup> Napoleon ensured that his proclamations were published in newspapers, posted on placards, and spread around adjacent countries to influence the civilian population of the Empire and European neighbors.<sup>[24]</sup> Hughes also claims that in addition to his widely disseminated proclamations, Napoleon used trusted agents to circulate his *Bulletin de la Grande Armée* throughout neighboring countries to influence foreign leaders and manipulate public opinion.<sup>[25]</sup> and dispersing bulletins to "justify France's involvement in the Napoleonic wars and mobilize support for the struggle against the Allies."<sup>[26]</sup> As evidenced, Napoleon's actions in the 19<sup>th</sup> century illustrated deliberate employment of MISO as a means of information warfare to leverage the informational element of the instruments of national power to achieve French strategic objectives, and to influence diplomatic, informational, military, economic and other social or infrastructural aspects of the operational environment.<sup>[27]</sup>

The foregoing 18<sup>th</sup> and 19<sup>th</sup> century examples of information warfare illustrate offensive-oriented forms of information-related capabilities. Information warfare also entails defensive-oriented activities designed to safeguard information which the Joint Force depends upon to conduct military operations. One such information-related capability is operations security (OPSEC), which JP 3-13.3 describes as a “capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.”<sup>[28]</sup> Napoleon’s method of disseminating military orders clearly demonstrated his attention to the OPSEC information-related capability. According to Baron de Jomini, for example, Napoleon delivered detached orders to his marshals in a way that prescribed “for each one simply what concerned himself, and only informing him what corps were to operate with him, either on the right or the left, but never pointing out the connection of the operations of the whole army.”<sup>[29]</sup> In this manner, Napoleon employed OPSEC by actively safeguarding critical information via a need-to-know method for orders dissemination. This was further emphasized by Jomini, who stated, “I have good reasons for knowing that he did this designedly, either to surround his operations with an air of mystery, or for fear that more specific orders might fall into the hands of the enemy and assist him in thwarting his plans.”<sup>[30]</sup>

Jomini noted that like Napoleon, Frederick the Great also actively practiced OPSEC measures to identify, control, and protect critical information associated with specific military operations and activities. Jomini illustrated this, reporting that “it is certainly of great importance for a general to keep his plans secret; and Frederick the Great was right when he said that if his night-cap knew what was in his head, he would throw it into the fire.”<sup>[31]</sup> As described, Napoleon and Frederick the Great both conducted defensive-oriented information warfare through the intentional employment of OPSEC as an information-related capability. History also confirms that these two 18th century leaders actively exercised OPSEC processes to prevent adversaries from garnering the information needed to assess friendly capabilities and intentions correctly.<sup>[32]</sup>

The preceding discussion makes it plain that the concept of information warfare was not born in the early 20<sup>th</sup> century. The basic ideas date back millennia. 18th and 19th century leaders operationally manipulated the information environment and leveraged other information-related capabilities to conduct information warfare against their adversaries. These leveraged information activities included intelligence gathering, military deception, military information support operations, and operations security.

Nonetheless, the proliferation and application of advanced technology has opened a Pandora's box in terms of the breadth and depth for which the information domain can expand and further impact (positively and negatively) the operational environment and leaders' understanding of it. As such, the rapid and widespread emergence of information-related capabilities and resulting cyber threats has profoundly altered the nature of information warfare, presenting extreme, complex challenges Joint Force leaders must meet if they are to dominate the multi-domain battlefield worldwide. As technological innovations continue, improved methods for conducting information warfare will emerge, especially with the continued revolutionary growth and scalability of techniques that leverage artificial intelligence. The key question that remains is whether the Joint Force will succeed in dominating the information environment in the physical, informational and cognitive dimensions.🛡️

**NOTES**

1. Department of Defense, *Joint Publication (JP) 3-13 Information Operations, Chg. 1* (Washington DC, 2014) I-1.
2. Headquarters, Department of the Army, *Field Manual (FM) 3-0 Operations, Chg. 1* (Washington DC, 2017) I-6.
3. *Ibid.*, 1-9.
4. Department of Defense, *JP 3-13 Information Operations*, I-1.
5. Jonathan B. A. Bailey, “The First World War and the birth of modern warfare,” in *The Dynamics of Military Revolution: 1300-2050*, ed. MacGregor Knox and Williamson Murray (New York: Cambridge University Press, 2001), 147.
6. Department of Defense, *JP 3-13 Information Operations*, II-10.
7. *Ibid.*
8. Christopher Duffy, *The Army of Frederick the Great* (New York: Hippocrene Books, Inc., 1974), 145.
9. *Ibid.*
10. *Ibid.*
11. Department of Defense, *JP 3-13 Information Operations*, II-10.
12. Duffy, *The Army of Frederick the Great*, 145.
13. Carl Von Clausewitz, “Intelligence in War,” in *On War*, ed. Michael Howard, trans. Peter Paret (Princeton: Princeton University Press, 1976), 117.
14. Department of Defense, *JP 3-13 Information Operations*, II-10.
15. *Ibid.*
16. Duffy, *The Army of Frederick the Great*, 146.
17. Department of Defense, *JP 3-13.4 Military Deception* (Washington DC, 2017) II-1.
18. Carl Von Clausewitz, “Cunning,” in *On War*, ed. Michael Howard, trans. Peter Paret (Princeton: Princeton University Press, 1976), 202.
19. *Ibid.*
20. *Ibid.*, 203.
21. Sun Tzu, “On The Art of War,” in *Roots of Strategy: The 5 Greatest Military Classics of All Time*, ed. Thomas R. Phillips (Mechanicsburg: Stackpole Books, 1985), 23.
22. Department of Defense, *JP 3-13.2 Military Information Support Operations* (Washington DC, 2017) I-2.
23. Michael J. Hughes, *Forging Napoleon’s Grande Armée: Motivation, Military Culture, and Masculinity in the French Army, 1800-1808* (New York: New York University Press, 2012), 29.
24. *Ibid.*, 30
25. *Ibid.*, 31.
26. *Ibid.*
27. Department of Defense, *JP 3-13.2 Military Information Support Operations*, I-1.
28. Department of Defense, *JP 3-13.3 Operations Security* (Washington DC, 2016) I-1.
29. Antoine Henri de Jomini (Baron de. Jomini), “Chapter VI. Logistics; or, the Practical Art of Moving Armies,” in *Summary of the Art of War*, originally published in French in 1836, trans. Capt. G. H. Mendell and Lieut. W.P. Craighill in 1862 (Rockville: Arc Manor, 2007), 193.
30. *Ibid.*
31. *Ibid.*
32. Department of Defense, *JP 3-13.3 Operations Security*, I-4.







# Data Privacy and Protection: What Businesses Should Do

---

Kiersten E. Todt

**D**ata privacy and protection should be priorities for every business, large or small, regardless of sector or geographic location. Data collection is now a critical component of all business operations, whether it is client data to perform a simple service or enterprise data to ensure operations of critical infrastructure. In today's operating environment and with the continued expansion of the digital economy, data are a critical corporate asset. Despite the functionality and importance of data, it is difficult to encourage businesses to protect data on their own.<sup>[2]</sup>

But, this data protection challenge does not mean the US should leap to regulation. When I served as the Executive Director of the independent, bipartisan Commission on Enhancing National Cybersecurity in 2016, the Commission examined how to secure the Internet of Things (IoT) devices, recognizing the increasing interdependencies that were growing at that time and which have only been growing exponentially since 2016. The Commission ultimately determined that the best approach was to allow market forces to create incentives for companies to secure IoT devices; companies would define their business case for why "secure to market" should trump "first to market." If those market forces fail and companies do not take appropriate steps to secure IoT devices, then regulation should be introduced.

Businesses find themselves singing this refrain as they struggle to secure today's digital economy. One primary obstacle is that businesses do not know how to evolve their thinking on security to align with trends in technology and innovation. They use traditional, historical models of thinking when it comes to security, models that previously had physical components at their core. This environment no longer exists. Digital infrastructure and digital interdependencies define our economy and our threat environment, creating challenges, like privacy, that require new thinking and new approaches.



**Kiersten E. Todt** is currently the President and Managing Partner of Liberty Group Ventures, LLC and advises senior executives and Boards on cyber risk management, including the development and execution of tabletop exercises; she also provides strategic advice and counsel to senior leaders in industry and government. She is the Managing Director of the Cyber Readiness Institute, which convenes senior leaders of global companies to help small and medium-sized enterprises improve their cybersecurity. Ms. Todt is the Scholar in Washington, DC of the University of Pittsburgh Institute for Cyber Law, Policy, and Security and most recently served as the Executive Director of the Presidential Commission on Enhancing National Cybersecurity. She has served in senior positions in the White House and in the United States Senate, where she drafted components of the legislation that created the U.S. Department of Homeland Security.

As businesses seek to understand how best to protect and secure data, we need to recognize and understand the influence of technology platforms, like Facebook, Google, Twitter, and YouTube, which are collecting and aggregating data at unprecedented rates and in exponential quantities than we have ever known. The US struggles to address the power of these technology platforms because we are not defining them accurately. These companies are not “just” technology platforms, as their General Counsel’s asserted on Capitol Hill in 2017 and their senior executives have done so repeatedly since then. These companies have become a sector critical to the functioning and security of our nation and must act with the responsibility and accountability that we demand of other sectors critical to our nation’s well-being.

Before 9/11, the US created categories of critical infrastructure, including telecommunications, finance, and energy, that the government determined were essential to our nation’s economic and national security. Even as the digital economy exploded over the past fifteen years, US security policies have continued to focus on these traditional industries. As interdependencies among infrastructure are growing, the lines defining what is and is not critical are blurring. The definition of critical infrastructure must evolve and align with the growth of the digital economy and its potential impact on our national security.

Technology platforms were developed to innovate, make actions easier, faster, more convenient, and to create global connections. But the technologies have grown at a rapid pace and are now much more ubiquitous than what their original business models intended them to be. Companies are beginning to acknowledge that with the power of their technologies comes newfound responsibilities. The cybersecurity failures of the last few years (e.g., Target, Sony, the U.S. Office of Personnel Management, Equifax, Marriott, Facebook) have forced the U.S. Government and businesses

to re-examine and re-define what is critical in today's environment. In the aftermath of these events, the importance of protecting critical information has become more apparent, yet, the nation continues to fail at making protecting critical information a priority.

Securing and optimizing privacy protection protocols around those data should be a critical function of any organization that holds data and, even more so, when a company holds sensitive data, such as personal DNA or personally identifiable information (PII). Traditional approaches to securing data typically have been driven by the mission of the organization and how it relates to protecting critical infrastructure. However, in today's environment, almost all organizations and businesses are part of a value chain connected to critical infrastructure. Therefore, data privacy and protection need to be a priority for all enterprises.

Many organizations are unaware that the data they hold can be access points to critical operations and functions, unrelated to their business. We cannot assume that all businesses that hold enormous amounts of critical data will voluntarily take the disciplined steps necessary to protect those data. The solution is two-pronged:

- 1) Companies need to be educated that, regardless of the mission of their organization (i.e., pizza parlor or public utility), some or even most of the data they hold are critical and needs to be protected. Companies have to make risk management decisions, based on their corporate mission and functions, regarding how much they invest protecting their data. A public utility, for example, will invest more in the protection and security of its data than a pizza parlor.
- 2) Companies must know the voluntary steps they can and should take to protect their data. All types of data are not equal. Companies need to understand the data they have and identify what is critical and what should be prioritized to ensure they are appropriately protected.

As large and small businesses worldwide try to understand the impact of the growing and interdependent digital economy, the European Union (EU) has stepped in with a heavy regulatory hammer. The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy that also addresses the export of personal data outside the EU and European Economic Area (EEA). Through this regulation, the EU has asserted that when it comes to security and privacy, organizations need regulation and the threat of stiff financial penalties to do the right thing. GDPR has been in effect for a year, and the world is learning from the European experience and beginning to look at data privacy and protection in the context of GDPR. Some US sectors already are using GDPR as a de facto standard. Additionally, the state of California worked off GDPR to shape the California Consumer Privacy Act, which was signed into law in June 2018 (effective in 2020). Under the GDPR, every business that brushes against the European Union has a privacy agreement.

GDPR forces companies to conduct due diligence on the data they hold and how they are protecting them. But it is not enough in the EU to be GDPR-compliant. As with most original drafts, GDPR needs editing, and it will take a while for the edits to be approved and then enacted. In the meantime, the secondary (negative) impacts of GDPR—on small businesses, on the necessary and vital collection and retention of threat data, to name a few—are growing.

What should companies be doing to protect privacy and data? Let's start with privacy. Privacy is a concept that, in the digital economy, has become jargon, and it is a concept that varies widely depending on the culture. For example, the US approach to privacy, which originated in the Bill of Rights, is much more liberal than that in other countries, such as Germany. The US has a broad range of what it will accept regarding data privacy, based on how that information is used. In the US and certain other western countries, some assert their desire for privacy, but what they are actually asserting is a desire for control over their information. Those who truly care about their privacy would not allow social media tracking applications that let others know where they are at any given moment or feel comfortable posting on the World Wide Web personal photos of and information on children or families in private locations. What many people in these countries care about is control of their data, not necessarily the absolute privacy of their data.

Prudent businesses that are mindful of these widely varying interpretations of privacy are creating a baseline level of privacy that protects the volumes of data they collect and retain. Before presenting approaches for protecting data, it is important to recognize that this aggregation of data at unprecedented rates in our world's history also means that an element of any efficient privacy policy and data protection policy should be the elimination of data that is no longer needed. Our muscle memory on data demands that we focus on data retention and on the concern that we will somehow lose data that we will need in the future. Because data accumulation often is unlimited, a critical component of data privacy and protection policies is the regular review of data that can and should be deleted. In the past, we were forced to shred paper when we no longer needed documents because of the restrictions of physical space. The dawning of digital files makes it too easy to keep everything, which becomes a significant risk to the protection and security of data. Developing a sound and active policy on data deletion is a salient and necessary part of any effective privacy and data protection policy.

The three critical elements of a comprehensive business data protection plan are:

- 1) data inventory;
- 2) public projection of data privacy and protection policies; and,
- 3) incident response.

### ***1. Data Inventory***

A key element of protecting data is developing and executing a thorough process for creating a data inventory that prioritizes the business data according to the business mission and sensitivity of data. Critical questions to ask and answer include:

- ◆ What data do you hold and where do you keep them (i.e., geographic location and relationships with partners, third-party vendors, and service providers)?
- ◆ Who can access your data?
- ◆ How are you using your data?
- ◆ Do you know where your data is held along your value chain?
- ◆ Do you track your data appropriately and effectively?
- ◆ What security protocols do your partners, third-party vendors, and product and service providers have in place?
- ◆ Can you consolidate where your data are held?
- ◆ What data can you delete on a regular basis?
- ◆ Do any of your vendors present too much risk?
- ◆ Do you have the proper controls in place? Do these controls reflect your data and asset priorities?
- ◆ What are your consumers/clients asking/demanding of you regarding data privacy and protection?
- ◆ What can (and should) be told to your consumers/clients regarding your data privacy and protection safeguards?

To protect and secure data, businesses must be organized. Businesses need to inventory and prioritize all of their data because it is difficult and costly to protect all data in the same way. Businesses should also pay close attention to administrative privileges and who has access to data, both within the organization and externally (i.e., third-party access). A key component of all human resources functions is a strict policy on the immediate removal of access privileges once an employee is terminated.

There should be certified contractual agreements with all third-party vendors that require a baseline of privacy and protection policies, which align with the business policies. A business needs to map the journey its data takes to understand the vendors it touches and to ensure data protection and privacy are maintained throughout the value chain. A business also needs to know its role in the value chains of other businesses. Additionally, as discussed before, a critical component of data protection is the regular and deliberate deletion of data that is no longer needed. Finally, business data protection policies must align with the demands of the consumer/client, which is why effective and continuous public protection of data privacy and protection is important.

### ***2. Public Projection of Data Privacy and Protection Policies***

In crisis communications, how a business communicates its response can be as important as the response itself. If a business inaccurately or ineffectively communicates how it responds, the public reaction can be destructive. Similarly, how a business communicates its prioritization of privacy and data protection policies and how that prioritization aligns with client/customer demands can be almost as important as the policies themselves. These policies cannot exist effectively in a vacuum; their interface with the public is critical to their success and effectiveness. A business needs to think deliberately about how its policies impact and are understood by the public – both in how the enterprise communicates the policies and how it chooses to engage with the public. For example: What privacy options are available on the business website? How much user engagement does a business have? How much attention does the business pay to fulfilling data requests? These factors all play important roles in how effective policies will be. Transparency and ensuring that customers and the public understand how their data are being used and how they are being protected is critical. Greater transparency leads to improved awareness and confidence in customers, which helps businesses serve these customers more effectively.

### ***3. Incident Response***

Repeatedly, businesses hear that experiencing a security breach is not a matter of “if” but “when.” In the current threat environment, most businesses have experienced some form of security breach. If proper policies are in place and if a resilient strategy for business security is well-executed, then a breach is not a demonstration of failure. In fact, success is more often measured not by what is prevented but by how effectively a business responds to an event. Was it possible to minimize disruption and prevent operations from going offline or, at a minimum, to contain the impact so that other functions were not disrupted? Developing a sound incident response plan is key to the success and effectiveness of privacy and data protection.

A business needs to identify the trigger points for communicating internally, including to its Board of Directors and to its customers and clients. These trigger points should be identified, in advance, to minimize the number of subjective judgment calls during an event. These decisions should be in line with customer expectations. When a crisis or event occurs, especially a significant one, first reports are often wrong. A business needs to have an internal agreement, ahead of time, on the protocols for public statements following an event. An effective template that can be drafted, pre-event, is a statement that outlines the actions the business has taken to be a resilient organization.

## **CONCLUSION**

Data privacy and protection should be priorities for every business, regardless of size, sector, or geographic location. A business needs to know its customers/clients understanding of privacy and what they expect of the business. Regarding data protection, a business should focus on three primary actions: data inventory, public projection of data privacy and protection policies and, incident response. By focusing on these actions, a business will develop a sound, resilient, and robust approach for data privacy and protection. It will also ensure an effective and strategic response when an incident does occur.♥





# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆



# How Could They Not: Thinking Like a State Cyber Threat Actor

---

Gregory Conti  
Robert Fanelli

## ABSTRACT

Information security and intelligence professionals have long known the value of thinking like their adversary. If the defender can put themselves into the mind of their adversary, they can predict behaviors, anticipate attacks, and make moves and counter-moves that frustrate their enemy at a level far beyond what a traditional reactive defense can accomplish. While much has been discussed about cyber threats in general, state actors are a special case with unique attributes. In the press we see coverage of state cyber operations, but only at the surface level. This article provides a more meaningful, and ultimately more useful, understanding of how state actors think, what incentives drive them, what challenges they face, and what special advantages state actors possess.

## INTRODUCTION

One of the most valuable information security skills is thinking like an adversary. However, not all adversaries are created the same. Defenders who do not understand how state cyber forces operate can come to false and potentially dangerous conclusions about the risks they face. Conversely, by knowing how a state cyber force thinks, their capabilities, bureaucracy, constraints, incentives, and ultimately how they view the world, we can develop better defenses against these the most capable of all threat groups.

© 2019 Dr. Gregory Conti, Dr. Robert Fanelli



**Gregory Conti** is Senior Security Strategist at IronNet Cybersecurity. Previously, he ran West Point's cybersecurity research and education programs for almost a decade and served in a career of intelligence and cyber operations assignments. He holds a PhD in computer science and has published more than 70 research articles covering cyber warfare, online privacy, usable security, and security data visualization. He is co-author of the recently published book – *On Cyber: Towards an Operational Art for Cyber Conflict*. Greg has served as Officer in Charge of a forward deployed expeditionary cyber team, acted as a Senior Advisor in the US Cyber Command Commander's Action Group, and co-created U.S. Cyber Command's flagship Joint Advanced Cyber Warfare Course (JACWC). He has spoken at numerous security conferences, including Black Hat, DEFCON, ShmooCon, RSA, and the NATO Conference on Cyber Conflict and numerous academic conferences. His work can be found at [www.gregconti.com](http://www.gregconti.com) and @cyberbgone

Having worked at both the National Security Agency (NSA) and U.S. Cyber Command (USCYBERCOM), the most valuable learning points for us weren't the tools and tactics of today's threat actors, but how they think. We saw a first-hand glimpse of NSA's Tailored Access Operations (TAO) in Rob Joyce's powerful USENIX Enigma talk two years ago. This talk gave us clues into how his team thought about cyber operations.<sup>[1]</sup> This article extends these insights by highlighting what makes state threat actors different, how they think, and how we can blunt their activities by crafting better defenses.

The line between the capabilities of state cyber forces and those of criminal groups is blurry. There are both sophisticated criminal groups and lousy state groups today. This has not changed. However, state cyber forces have unique capabilities that criminal groups do not possess. States employ the full extent of national power in ways even the most sophisticated criminal groups simply cannot.

Tools like the Center for Internet Security's Top 20 Controls and the NIST Cybersecurity Framework are effective means to help construct defenses against the most common 80% of threats.<sup>[2]</sup> However, the CIS Top 20 and NIST Cybersecurity Framework<sup>[3]</sup> alone will not stop the dedicated and well-resourced state actor. Covering that 20% gap is the true challenge. While we aspire to perfect security, we can never reach it, even with extensive resources and attention. We can, however, accomplish much by understanding the state threat and crafting our defenses accordingly.

Of course, no two nations are the same. How a liberal democracy thinks about cyber operations may differ greatly from an authoritarian regime. Even within these general classes, the unique attributes of each country, its culture, and its objectives may vary dramatically. To account for the differences, we have distilled underlying principles that are broadly applicable.



**Robert Fanelli** is a computer scientist and security practitioner with IronNet Cybersecurity. Prior to joining IronNet, he served as a US Army Colonel at U.S. Cyber Command in multiple roles, including controlling DoD global cyberspace operations, leading the USCYBERCOM/NSA Combined Action Group and conducting research and development activities. He has published, presented and taught security topics in several venues, including the United States Military Academy at West Point and the National Cryptologic School. He holds a PhD in Computer Science from the University of Hawaii, MS from the University of Louisville, a BS from Penn State University, and several industry credentials, including the designation of GIAC Security Expert (GSE).

### *State Activities Aren't Always State-Only*

We tend to think of state cyber operations as unilateral activities, but the reality is more complicated. Operations may be state-operated, state-sponsored, state-affiliated, or state tolerated.<sup>[4]</sup> States may prohibit, ignore, encourage, shape, coordinate, order, or execute cyber activities.<sup>[5]</sup> As these nuanced relationships imply, partnerships, either willing or coerced, are common.

A state may provide targeting data to patriotic hackers, immunity to criminal groups, advanced tools to mercenaries, protect a leaker from extradition, or collect intelligence via state-owned technology companies. By operating through explicit or implicit partnerships states hinder attribution and gain plausible deniability for their activities. Expect partnerships between states and less capable, often disposable, threat actors. When you see non-state groups conduct cyber operations with an unlikely degree of sophistication, consider if there is a state benefactor behind the scenes.

### *State Actors Can Be Unreasonably Tenacious*

State backing provides advantages that permit state actors to explore further, delve deeper, and persist longer than other actors in pursuit of their objectives. The assertion that a strong enough defense will dissuade attackers and induce them to go elsewhere in search of a softer target will not hold up when targeted by state actors.

State sponsorship provides more extensive access to hardware, software, infrastructure, and other resources needed to conduct operations. State actors can apply these resources to find and exploit vulnerabilities that other actors would bypass as being too difficult or uncommon to be worth the effort. State actors can also apply resources to conduct coordinated operations on multiple targets simultaneously. A single successful operation may be enough to achieve the overall objective. Further, resources expended during operations can be more easily replaced, allowing state actors to keep coming back long after other actors would become significantly impaired or defeated altogether.

Many cyberspace actors conduct their activities on a part-time basis, needing to engage in other work to pay the bills. More committed criminal actors may make a living from their activities, but they must make a profit or move along to another target. State actors have jobs too: to accomplish the state's objectives. Having the bills paid allows these actors to persist in gaining and maintaining access to a target long after the other actors would give up in search of more lucrative opportunities.

Although the potential for profit may not be immediately obvious to defenders, criminal actors typically conduct their operations with some sort of financial gain in mind. Unprofitable operations do not pay the bills and will be discontinued. State actors can pursue extensive operations with no opportunity for financial gain because profit is not the objective.

A tenet of information system security is that should a vulnerability exist, sooner or later an intruder will find and exploit it. State actors have the tenacity to find and exploit vulnerabilities in ways, and over time frames, that are not feasible for others.

### *States Create Vulnerabilities*

Most attackers use pre-existing vulnerabilities to conduct their attacks, more sophisticated attackers find new vulnerabilities to exploit, but the most sophisticated—state attackers—will create their own vulnerabilities.<sup>[6]</sup> State actors use publicly available tools and techniques first. Public techniques are cost effective, reduce the chance of attribution, and avoid leaking sensitive tradecraft. Using a novel capability is expensive and risks revealing the attack, mode of operation, and providing incriminating clues for attribution.<sup>[7]</sup> Copycat tools and resistant defenses would soon follow.

At the next tier, states discover new vulnerabilities. While independent hackers may perform vulnerability discovery,<sup>[8]</sup> the key difference is scale, scope, and access to prohibitively expensive gear, such as x-ray machines, electron microscopes, and other equipment needed to emulate their target. While a small group of hackers seeking to identify vulnerabilities might purchase used parking meters on discounted websites,<sup>[9]</sup> they could not muster the resources to build a small nuclear centrifuge facility.<sup>[10]</sup> Sophisticated states employ massive vulnerability discovery efforts, such as employing contractors who specialize in large scale fuzzing, paying large sums of money to bug bounty hunters, and acquiring access to proprietary source code and hardware designs.

States are effectively unique at the highest tier—creating vulnerabilities. Such activities are rarely attributed publicly, but we see echoes and accusations reported in the press. For example the US banned the use of Kaspersky technologies in the federal government due to concerns over Kremlin influence.<sup>[11]</sup> The long-standing tension between the US government and Chinese technology companies ZTE and Huawei come from similar concerns.<sup>[12]</sup> The US government has been accused of deliberately weakening the Data Encryption Standard (DES)<sup>[13]</sup> and paying a security vendor \$10M to weaken its flagship security product.<sup>[14]</sup>

State actors exploit privileged relationships with companies under their influence. Such relationships can lead to supply chain attacks that compromise hardware or software before the technology even leaves the factory. Even if the company is unwilling, access to desirable markets is another a means of creating vulnerability. For example, to comply with China's cybersecurity laws, Apple moved iCloud cryptographic account keys and customer data into China.<sup>[15]</sup> Similarly, Google moved servers and user data to Russian data centers to comply with Russian law.<sup>[16]</sup> We should assume states will maneuver security sensitive devices, people, hardware, software, companies, standards, and information to create vulnerability.

### *State Cyber Forces Will Push the Limits of Authority*

State cyber forces want to aggressively do their jobs and will push their authorized activities to the limit, and then ask for greater authority.<sup>[17]</sup> A good analogy is that of a guard dog: the guard dog will strain against its chain. Give it a longer chain—sometimes wise and sometimes unwise—and it patrols a larger area. Many of these legal authorities will not be publicly acknowledged, but quietly overseen by government officials.<sup>[18]</sup> There is a difference between “legal” and “front page of the New York Times legal,” though, so some legal authorities may be undermined or eliminated if they become public.

### *Going Off Script Can Get Operators Reprimanded, Banished, Imprisoned...or Promoted*

Whether long or short, every government has a leash on its cyber forces. The degree varies by the type of government and affects both operations and the personal lives of operators. Failure to comply invites punishments that vary based on culture and rule of law. In law-abiding democracies, we'll see career terminations, reassignments, and arrests. In strict regimes, we'll see more severe punishments, including execution. As an example, German hacker, Karl “hagbard” Koch, who allegedly worked for the KGB, was found burned to death after a computer espionage operation ended badly.<sup>[19]</sup>

In traditional military operations, the US employs the Mission Command paradigm, which pushes authority and responsibility down to those at the front lines, which creates great agility and responsiveness. In contrast, the Soviet military maintained tighter hierarchical control, limiting their agility. Today, the US maintains tight control of cyber operations while many other threat actors maintain a looser degree of control. With less control, cyber operations can be executed and adapted more rapidly.

Cyber force personnel are also under control and observation. The more sensitive the work of an individual, the more intense the scrutiny. It is common to require operators to undergo extensive and reoccurring background checks and polygraph exams. As the frequency of these checks may be insufficient, the US is exploring continuous monitoring of clearance holders—checking such things as court proceedings, financial data, and credit scores for anomalies in near real time.<sup>[20]</sup>

Not all failure ends in doom. “Fail fast” is a philosophy common in Silicon Valley and is increasingly fashionable in militaries. Innovation is necessary for success in cyber conflict and innovation can’t flow when organizations are rigid and risk adverse. At a recent cyber conflict panel, Katie Moussouris asserted that, “we need rule-following rule breakers.”<sup>[21]</sup>

Hierarchical bureaucracies don’t readily embrace innovation and rule breaking, but those that do gain the advantage. The US does not possess a monopoly on innovation. As the secrecy of the Democratic National Convention hack unraveled, those behind the operation agilely created the Guccifer 2.0 persona to share the leaked documents—turning the beginnings of a defeat into a victory. We are seeing a shift in the cyber activity in Asian countries move from intellectual property theft to entrepreneurship. We should expect increasing innovation from the state cyber forces of all countries.

No government likes to be embarrassed by its cyber operations. With flexibility comes innovation, but also risk. Because of the risks, expect a playbook of authorized activities and step-by-step scripts of actual operations from nations that enact strict control. In nations employing looser command and control, there will still be boundaries, such as avoiding hacking internal to the country and avoiding embarrassment to government officials.

### ***State Actors Challenge Fundamental Security Assumptions***

State cyber actors adeptly exploit security assumptions. We all make assumptions about the security of our systems, the risks we face, and threat actor abilities. When our assessment is off, we can expect a bad day. For example, most users assume their web communications are secure. In actuality, web security is based on cryptographic certificates embedded in our browsers. This assumption proved dangerous in 2011 when a state threat group breached Dutch certificate authority, DigiNotar, issued fraudulent certificates and conducted a large-scale man-in-the-middle attack against Iranian Gmail users.<sup>[22]</sup> Another core security technology, code signing, designed to prove authorship of software, was similarly utilized to create authentic appearing, but malicious software.<sup>[23]</sup> According to press reports, state actors may have created sham academic conferences to lure potential defectors,<sup>[24]</sup> installed malware in hard drive firmware,<sup>[25]</sup> partnered with chip manufacturers to create hidden back doors, and threatened undersea telecommunication cables with submarines.<sup>[26]</sup> Whether these specific examples, supply chain attacks, compromising insiders, or something that we have yet to consider, states will not necessarily fight “fair”—even if at the cost of the broader security ecosystem. We must carefully consider the security and trust assumptions we make about state threats.

### ***States Actors Have Strategies; We Have Tactics***<sup>[27]</sup>

Sophisticated state actors execute long-term plans, while most defenders are perpetually stuck in near-present tactics. State strategies aim for long-term objectives, like creating division in the US or undermining US dominance in the world. Multiple supporting operations and campaigns,<sup>[28]</sup> cyber and otherwise, support the implementation of such strategies. Leaders in



democratic governments—those charged with lasting strategy—have difficulty creating long-term defensive programs. Each politician’s influence is at risk every election cycle so long-term planning suffers. The private sector often suffers from similar limitations, as the average tenure of corporate security executives and directors hovers around 2.5 years.<sup>[29]</sup>

Short range thinking at both the enterprise and national-level hinders defense. We often hear of a looming cyber-Pearl Harbor, but a death-by-a-thousand-cuts scenario is happening now. Patient threat actors operate below a threshold of national response—the type of attacks that cause damage or public outcry that demand a response. Consider the U.S. Office of Personnel Management (OPM) hack of 2015. Significant as it was, years later little has changed.<sup>[30]</sup> Accountability in the private sector is not much different. A year after the Equifax hack, the company has yet to face serious consequences.<sup>[31]</sup>

Government lethargy gives state attackers the space to execute strategies over years. Occasionally actors do cross the line and generate more than a token response. But these incidents are rare. Russian influence operations during the US presidential election clearly got the attention of policymakers, but even so, the wheels of government turn slowly. Absent a painful and long-lasting deterrent, threat actors continue with their long-term plans. Success emboldens future audacious activity.

Expect long-long term planning conducted by professional cyber operators, intelligence analysts, and military planners. Some plans are used immediately, while others sit on the shelf until needed. Central to the success of many cyber operations is privileged access to target computing systems. Governments will cultivate such access over many years. Some access will be used to quietly gain intelligence and others will be maintained for later use in time of crisis or opportunity. State actors conduct systematic reconnaissance to keep their plans fresh. Analysts will use intelligence community tools like Center of Gravity<sup>[32]</sup> analysis, which breaks anything down—from a country to a sector to an enterprise—into vulnerable parts, to build prioritized targeting lists. These lists guide intelligence collection efforts and offensive action. The acquisition of access and the conduct of surveillance occurs continuously as do cyber operations that fall below the threshold of an organized response.

Defenders cannot play checkers while adversaries are playing chess. States execute synchronized strategies across many playing boards: political, economic, informational, social, and technical, and plan many moves ahead.

### ***States Think at Massive Scale***

States think big. When individuals and small groups can quickly create tools that scan the entire internet in minutes (MassScan),<sup>[33]</sup> massive databases of compromised accounts (Have I Been Pwned),<sup>[34]</sup> a hardware-based code cracking machine (DES Cracker),<sup>[35]</sup> a search engine for internet-connected devices (Shodan),<sup>[36]</sup> a platform for easily organizing and employing computer exploits (Metasploit),<sup>[37]</sup> and a small computer program that combines Metasploit

and Shodan into a weaponized targeting and exploitation platform (Autosploit),<sup>[38]</sup> we should assume sophisticated states are more capable by an order of magnitude or more.

Ask yourself what could you do with a billion-dollar budget, a robust intelligence apparatus, a cyber army, and sovereign immunity? Maybe repeatedly map the entire Internet, create special forces-like A-teams for offensive and defensive operations, develop a global targeting database, call every phone number on the planet looking for connected technology and vulnerable humans, optically scan the outside of every piece of mail in a postal system, weaponize artificial intelligence, compromise election infrastructure, work with printer vendors to place covert microdot serial numbers on printouts, use submarines to probe undersea cables,<sup>[39]</sup> or plant malware in critical infrastructure. Or maybe, steal a database of every security clearance holder in a country (OPM Hack), combine it with their travel records (United Airlines Hack) and medical health information (Anthem Hack), and then build a Facebook-like interface for easy navigation by your spies and cyber operators?<sup>[40]</sup>

Those who think they aren't a state target are wrong. If you are doing something of value, you are on a state targeting list. If you are really interesting, like a critical infrastructure company or a senior official, you'll get extra attention.

### ***States Have Security Research Ahead of the Open Community***

Much state security research occurs behind closed doors. We should assume that state cyber forces are five to ten or more years ahead in cryptography and offensive security. One famous example is that of public key cryptography. From 1970-1973, the UK's GCHQ covertly developed public key cryptography. Academic researchers later discovered public key cryptography in 1976. GCHQ's classified discovery did not become known until it was declassified 27 years later.

Governments invest billions into classified and unclassified research programs. US programs like DARPA's Cyber Grand Challenge<sup>[41]</sup> used AI to attack and defend machines and the Neural Engineering System Design program which seeks direct communications between digital technology and the human brain.<sup>[42]</sup> Not all countries have the will or resources to fund such massive programs, instead they may simply steal the intellectual property. We should assume foreign cyber powers have well placed faculty members and students across US academic institutions, seek to place agents in private sector companies, and use leading information security conferences to gather information and recruit.

While classified programs lead in many areas, especially offense, private industry leads in others. Many top companies have well established operational cyber defense programs that provide best practices. That said, less well-resourced small and mid-sized companies lag behind these benchmarks, as does much of the government sector outside of the defense and intelligence communities.

We must move beyond US overconfidence and assume we will not enjoy a perpetual lead in many emerging technologies. For example, China has made major advances in quantum computing,<sup>[43]</sup> supercomputing, and artificial intelligence and now rival these technologies in the US. We should expect more.

### ***States Leverage the Full Spectrum of National Power***

State cyberspace operations do not exist solely in a technical-only vacuum. Governments employ their full spectrum of tools including diplomatic, informational, economic, law enforcement, and military levers of power to achieve their objectives. A state might ban use of foreign-made technologies or track funding behind suspicious technology transfers, require a tech titan's data be hosted in their country, and exploit state-owned businesses to gain privileged access to data, product specifications, and emerging technologies. Militaries will complement cyberspace operations with air, land, sea, space, electronic warfare, and information operations forces. States possess robust intelligence agencies with global human intelligence, signals intelligence, imagery intelligence, and other collection programs to inform current cyber operations and prepare for future conflict. States can selectively create, enforce, or ignore their laws. A government could issue a state department demarche, create fake passports and manufacture identities, or represent their equities in international policymaking forums. All of these are capabilities out of reach of traditional cyber threat actors. Thus, cyberspace operations themselves will also take place in multiple planes, buttressed by the full range of tools available to national governments.

### ***State Forces Aren't Superhuman***

Although we recognize and have addressed many of the strengths of state cyber forces, but these forces are not ten feet tall and bulletproof. Cyber forces today are in fact fragile; they are composed of people with rare talent, operating under intense pressure, and competing for scarce resources.

With size comes bureaucracy, and with bureaucracy comes friction. As a threat actor's size grows, it becomes unwieldy, and efficiency suffers. Here are some examples. Cyber exploits provide a competitive edge and organizations may overclassify their most valuable capabilities to prevent use by internal rivals. Established institutions, such as land and air forces, may see cyber forces as competitors who threaten their power, prestige, personnel, and funding.

Cyber forces are composed of humans and will struggle to attract, train, and retain talent.<sup>[44]</sup> Good people will leave, get sick, fail a physical fitness test, burn out, have babies, be skipped for promotion, lose their security clearance, or get enticing job offers outside government. Technically talented operators will become frustrated by spending long hours creating briefings to justify their missions. Criminal indictments will dissuade talent from participating in missions.<sup>[45]</sup> Leaks and compromises will hurt morale and damage public opinion.

Building cyber armies takes time. From the initial directive to create USCYBERCOM in 2009, it took until 2018 for the 133 teams of the command's Cyber Mission Force (CMF) to be fully operational.<sup>[46]</sup> And this was fast: it was jumpstarted by partnering with NSA and a pool of ready military and civilian talent that existed, in part, due to NSA's Centers of Academic Excellence program established in 1999. During the nine years from inception of USCYBERCOM to a fully operational CMF, the geopolitical and technical landscape shifted continually but the "under construction" force was conducting operations throughout this period. The takeaway: read reports of countries creating cyber armies seemingly overnight with a skeptical eye.

Government agencies—and the teams within agencies—do not necessarily talk to each other. Communication between cyber organizations, kinetic forces, and policymakers will remain problematic as each group struggles with need-to-know security considerations and a lack of shared vocabulary. The churn in civilian and military senior leadership means cyber operators must regularly re-educate and justify their activities to new leaders.

No nation is immune to the effects of politics. Politicians will inject politics into cyber activities—from funding to base locations to legal authorities to oversight. Some good people won't get promoted because they angered the wrong politician, and some less qualified people will be promoted because they have befriended the right person in power. Embarrassing a policymaker will negatively impact cyber activities and threaten cyber leaders; successes will gain accolades.

All governments are ultimately accountable to their populations. Cyber operations may be unpopular, especially those that involve surveillance and privacy. Undermining popular support can undermine governmental cyber operations. Due to the sensitive nature of cyber operations, compounded by a culture of secrecy, many cyber organizations struggle to communicate with their populations and the global audience. Reality on the inside may differ substantially from what is seen in the press.

State cyber forces are at a cultural disadvantage. Foreign adversaries are by definition, foreign. Cyber forces often do not possess the language skill of their targets. In fact, they need to maintain a diverse set of language skills sufficient for each target country, which is no easy feat. Language skills are highly perishable and subtle nuances in language can give away deception attempts. We have all seen this in email spam. Additionally, foreign adversaries lack the deep knowledge of a target country's culture. Experts in desired language and culture may exist, but they are always limited in number.


Finally, operational secrets rarely remain secret. The use of each capability leaks insights to the target, sometimes even a blueprint of the code itself. Cyber tradecraft and tools will be reverse engineered, copied, and improved upon. Obfuscation techniques are not bulletproof. We even see clues of threat actor bureaucracy in malware.<sup>[47]</sup>

## CONCLUSIONS

All too often we underestimate the goals, capabilities, resources, tenacity, and time horizons of state threat actors. The standard best practices espoused by NIST and the CIS Top 20 are an excellent start but fall short of proper state-grade defenses. We can address this gap in a variety of ways:

- ◆ **Urgency** – We need to avoid the complacency associated with partial solutions and move with a sense of urgency toward strong defenses.
- ◆ **Collective Defense** – Individual companies can't take on state actors individually. Even if one company has strong defenses, a state will patiently probe the business' entire ecosystem, or even the entire business sector, seeking a point of vulnerability until they find one. We need network visibility, automated information sharing, and security orchestration between companies, sectors, and governments to provide a comprehensive defense.
- ◆ **Public/Private Partnership for the Offense** – For most companies, it is illegal to hack back. Regardless of legality, corporate hacking back is unwise. Governments possess a monopoly on the use of force and public/private collaboration is necessary to strike back using the full spectrum of governmental power. A solid collective defense foundation will allow high-speed, automated requests for government support.
- ◆ **Realistic, Informed Assumptions** – Recalibrate your security assumptions using an informed and justifiably paranoid view of state threats.
- ◆ **Organizational Agility** – Smaller, more agile groups with less systemic friction will respond faster than a large hide-bound force. We must work to reduce bureaucratic friction to increase agility and improve morale.
- ◆ **Move Beyond Signature-based Security** – Sophisticated adversaries today avoid detection by signature-based security systems. We need more advanced technologies that detect threat behaviors. While it is easy to bypass signatures, it is much more difficult to bypass a behavioral detection system, such as network behavioral analytics. Deception technologies provide another powerful technique. You own the network, exploit your home field advantage.
- ◆ **Cyber National Training Centers** – Governments and companies need to learn how to fight in cyberspace as a cohesive whole. This requires common doctrine, interoperability, information sharing, regular exercises, and trust. Look to the U.S. Army's National Training Center<sup>[48]</sup> as a model for building strong integrated teams from disparate parts.
- ◆ **Military Strategy and Tactics** – Traditional information security controls are insufficient. State cyber forces are far more capable and organized to be deterred by these limited defenses. There are literally armies operating in cyberspace, and armies conduct cyber operations at scale. We must selectively draw from military doctrine for best practices to defend at scale.<sup>[49]</sup>

Once computing was the domain of hobbyists and well-intentioned hackers. Those days are long past. Cybersecurity today is serious business. Nations compete for dominance, and cybersecurity is looking a lot more like warfare, and business as usual is simply insufficient. No company can stand alone against state threat actors. Ignoring that states are active in cyberspace will not make the problem go away. For all their strengths however, state threat actors do possess weaknesses we can exploit. The CIS Top 20 Controls and the NIST Cybersecurity Framework provide the foundation for a credible defense, but they are insufficient alone. An urgent and rapid response that factors in state actors is necessary. We must learn to defend as sectors and nations in tight coordination.

Learning to think like a state actor is the fundamental first step. For defenders, the most important takeaway for understanding a state actor isn't "would they do it" or "could they do it," but instead, "how could they not?"

### **DISCLAIMER**

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, Department of the Army, Department of Defense, the National Security Agency, U.S. Cyber Command, the United States Government, IronNet Cybersecurity, or any other current or past employer.

## NOTES

1. Rob Joyce, “Disrupting Nation State Hackers,” USENIX Enigma, 2016, <https://www.usenix.org/node/194636>. See also, Rob Joyce, “NSA Talks Cybersecurity,” DEFCON, 2018.
2. “CIS Controls,” Center for Internet Security, <https://www.cisecurity.org/controls/>.
3. “Cybersecurity Framework,” National Institute of Standards and Technology, <https://www.nist.gov/cyberframework>.
4. Mara Tam, Twitter, August 29, 2018. <https://twitter.com/marasawr/status/1034856944090206208>
5. Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” Atlantic Council, January 2012.
6. U.S. Department of Defense, “Resilient Military Systems and the Advanced Cyber Threat,” Defense Science Board Task Force Report, 2013.
7. The use of a novel capability is sometimes called a “use-it-and-lose-it OPSEC risk.”
8. Sean Michael Kerner, “Critical Bug Bounty Reports on the Rise, HackerOne Finds,” eWeek, July 12, 2018.
9. Joe Grand, Jake Appelbaum, and Chris Tarnovsky, “Smart Parking Meter Implementations, Globalism, and You: aka Meter Maids Eat Their Young,” DEFCON, 2009.
10. Kim Zetter, Countdown to Zero Day, Broadway Books, 2015.
11. Dustin Volz, “Trump signs into law U.S. government ban on Kaspersky Lab software,” Reuters, December 12, 2017.
12. Ginger Gibson, “U.S. House passes defense bill targeting Chinese investments,” Reuters, July 26, 2018.
13. Bruce Schneier, “The Legacy of DES,” Schneier on Security, 2004.
14. Dennis Fisher, “RSA Denies NSA Backdoor Payment Allegations,” Threatpost, December 23, 2013.
15. Mikey Campbell, “Apple to move Chinese iCloud keys to China servers, opens door to government data requests,” AppleInsider, February 23, 2018.
16. Olga Razumovskaya, “Google Moves Some Servers to Russian Data Centers,” Wall Street Journal, April 10, 2015.
17. Dakota Rudesill, “Trump’s Secret Order on Pulling the Cyber Trigger,” Lawfare, August 29, 2018.
18. Alex Boutilier, “Canada’s electronic spies will be able to launch cyber attacks with little oversight, report warns,” The Star, December 18, 2017.
19. Cliff Stoll, The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, 2005.
20. Patrick Tucker, “US Plans ‘Continuous Evaluation’ of New and Existing Security Clearances,” Defense One, July 12, 2018.
21. Adin Dobkin, “Army pushes recruiting and retaining cyber talent,” Defense Systems, November 8, 2017.
22. Dennis Fisher, “Final Report on DigiNotar Hack Shows Total Compromise of CA Servers,” Threatpost, October 31, 2012.
23. Dan Goodin, “Stuxnet-style code signing is more widespread than anyone thought, ArsTechnica, November 3, 2017.
24. Daniel Golden, “How the CIA Staged Sham Academic Conferences to Thwart Iran’s Nuclear Program,” ProPublica, October 10, 2017.
25. Sean Gallagher, “How hackers could attack hard drives to create a pervasive backdoor,” ArsTechnica, February 18, 2015.
26. Garrett Hinck, “Evaluating the Russian Threat to Undersea Cables,” Lawfare, March 5, 2018.
27. Derived from Jeff Moss’ comment “our adversaries have strategies, we have tactics” in Black Hat USA Keynote Introduction, 2018.
28. Richard Bejtlich, “Elevating the Discussion on Security Incidents,” TaoSecurity Blog, February 19, 2015.
29. “Understaffed and at Risk: Today’s IT Security Department,” Ponemon Institute, February 2014.
30. Lee Mathews, “Office of Personnel Management Still Vulnerable 3 Years After Massive Hack,” Forbes, November 15, 2018.
31. Zack Whittaker, “A year later, Equifax lost your data but faced little fallout,” TechCrunch, CNET, September 8, 2018.
32. Dale Eikmeier, “The Center of Gravity: Still Relevant After All These Years,” Military Review, May 11, 2017.
33. Robert Graham, MassScan, GitHub.
34. Have I Been Pwned, <https://haveibeenpwned.com/>.
35. “EFF DES Cracker Machine Brings Honesty to Crypto Debate,” Press Release, Electronic Frontier Foundation, August 9, 2016.
36. Shodan, <https://www.shodan.io/>.
37. Metasploit, <https://www.rapid7.com/products/metasploit/>.
38. Teri Robinson, “Autosploit marries Shodan, Metasploit, puts IoT devices at risk,” SC Magazine, January 31, 2018.
39. Morgan Chalfant and Olivia Beavers, “Spotlight falls on Russian threat to undersea cables,” The Hill, June 17, 2018.



## **NOTES**

40. The Grugq, "A Short Course in Cyber Warfare," Black Hat Asia, 2018.
41. "DARPA Celebrates Cyber Grand Challenge Winners," Press Release, DARPA, August 5, 2016.
42. "Bridging the Bio-Electronic Divide," Press Release, DARPA, January 19, 2016.
43. Martin Giles, "The man turning China into a quantum superpower," MIT Technology Review, 19 December 2018.
44. Josh Lospinoso, "Fish Out of Water: How the Military is an Impossible Place for Hackers, and What To Do About It," War on the Rocks, 12 July 2018.
45. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Press Release, U.S. Department of Justice, May 19, 2014.
46. "Cyber Mission Force achieves Full Operational Capability," Press Release, U.S. Cyber Command, May 17, 2018.
47. Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," Smithsonian Magazine, April 2012.
48. Mario Hoffman, "Modernizing the Army's OPFOR program to become a near-peer sparring partner," Army.mil, October 1, 2018.
49. Gregory Conti and David Raymond, "On Cyber: Towards an Operational Art for Cyber Conflict, Kopidion Press, 2017.







# The Untold Story of Edward Snowden's Impact on the GDPR

---

Hallie Coyne

## INTRODUCTION

In June 2013, National Security Agency contractor Edward Snowden released a trove of information on classified U.S. Government surveillance methods. U.S. Intelligence chiefs warned that the ripple effects of the leak would be devastating and extensive. Five years later, in June 2018, Joel Melstad, a spokesman for the U.S. National Counterintelligence and Security Center, reported that Snowden's disclosures "have put U.S. personnel or facilities at risk around the world, damaged intelligence collection efforts, exposed tools to amass intelligence, destabilized U.S. partnerships abroad and exposed U.S. intelligence operations, capabilities and priorities."<sup>[1]</sup> Snowden's attorney, Ben Wizner, believes that these reports are exaggerated and alarmist, arguing that "the mainstream view among intelligence professionals is that every day and every year that has gone by has lessened the value and importance of the Snowden archives."<sup>[2]</sup> However, Wizner's assessment is regrettably limited in its scope. Importantly, it fails to account for the significant impact that Snowden's leaks had on the development of the European Union's General Data Protection Regulation (GDPR)—a piece of legislation that has fundamentally changed the nature of data privacy in the EU, and the world over.

The connection between Edward Snowden and the GDPR can actually be traced back to the European Parliamentary Committee on Civil Liberties, Justice and Home Affairs<sup>[3]</sup> (LIBE). This committee has a surprising history because, though its members were exceptionally interested in Snowden's leaks, its ensuing legislative activity has been largely understudied. For example, on October 29, 2013, then-U.S. Director of National Intelligence, James Clapper, appeared before the U.S. House Intelligence Committee to discuss Snowden's revelations.<sup>[4]</sup> The very next day, LIBE representatives met with senior National Security Council officials at the White House.<sup>[5]</sup> LIBE had an expansive mandate,<sup>[6]</sup> an entrenched concern for personal data protection,<sup>[7]</sup> and a history of treating national intelligence services with suspicion if not outright hostility.



**Hallie Coyne** is a recent graduate of the Frederick S. Pardee School of Global Studies at Boston University. While at BU, Ms. Coyne studied International Relations and History, with concentrations in International Security, and European Politics. She has been a research assistant on various projects investigating the European Union's institutional history. Ms. Coyne's research interests include transatlantic relations and the future of national security at the intersection of intelligence and emerging cyber capabilities. Before graduating, Ms. Coyne completed internships with the U.S. Embassy in Ottawa, via the Virtual Student Federal Service program (VSFS), and the International Trade Administration, within the U.S. Department of Commerce. She spent a semester at Sciences Po and later attended the Cambridge Security Initiative's 2018 International Security and Intelligence summer program (ISI), where she initiated the research for this paper. Ms. Coyne currently lives in the Washington D.C. area and works in the private sector.

Yet even with this robust background, LIBE operated with remarkable inconspicuousness.

Much of the current academic literature<sup>[8]</sup> overlooks or ignores the influence of the Snowden leaks on the functioning of the LIBE committee, and by extension, the formation of the General Data Protection Regulation.<sup>[9]</sup> This paper aims to introduce a new facet to the political contextualization of GDPR, by examining LIBE's pattern of framing data privacy issues in relation to the activity of security services that impact EU citizens. Prior to 2013, LIBE pursued power maximization efforts, exercising some method of informal control over the intelligence services of EU member states, and promoting data privacy and protection. After Snowden's leaks of U.S. intelligence capabilities, LIBE members capitalized on the opportunity to advance many of their goals. Given the breadth of GDPR, and the intentions of its authors, Ben Wizner's estimation of Snowden's dwindling relevance may prove acutely premature.

#### *Methodological and Theoretical Approach*

By using a historical review, this paper provides a long-range view of LIBE's engagement with the balance that exists between the EU and its member states at the intersection of data privacy and national security. This paper will not discuss the substantial scholarly work theorizing the development of the EU in its entirety. Similarly, theories in intelligence studies, pertinent though they may be, are beyond the scope of this investigation. A more substantial and analytical approach to address these issues certainly merits further study.

With such limitations in mind, a theoretical basis is still necessary to examine how LIBE's activities might be understood within its existing institutional framework and its broader international context. The traditional challenge of analyzing LIBE's activities via applying state-centric theories is inherent in the very existence of LIBE in the supranational body of the

European Parliament. This is considered a possible explanation for LIBE's comparative anonymity in the many studies completed with the intention of gauging the impact of Snowden's actions because "state-centric theories make it difficult for analysts to detect European [EU] foreign policy on their radars, and they are therefore bound to reject the existence or significance of European foreign policy."<sup>[10]</sup>

Therefore, the primary analytical framework applied to this historical review is drawn from theories of European integration. Such theories contextualize and seek to explain the behavior of EU institutions and their components. The theory employed is neofunctionalism, and the spillover process it implies. There are three widely accepted dimensions of the concept of spillover, all of which are applicable to this analysis. First, in functional spillover, the "core argument in relation to EU foreign policy is that, as internal policies become integrated, there is also pull towards developing an external dimension."<sup>[11]</sup> Second, political spillover suggests that as the EU integration process continues, "actor perceptions of state interests become increasingly European, focusing more on common interests."<sup>[12]</sup> Finally, and most importantly for the purposes of this paper, "institutions created by states have interests in pushing for more integration, termed cultivated spillover."<sup>[13]</sup>

GDPR is an extension of EU integration because it further harmonizes EU standards for data protection. For example, other dimension of EU policy certainly influenced GDPR's development. This paper specifically examines how the LIBE Committee's work on GDPR translated in part from its parallel interests and activities in the field of EU security policy. The following historical review traces the relevant activities of LIBE to the point of the Snowden leaks, evaluates the extent to which LIBE adjusted its legislative activity in the development of GDPR as a result, and argues that the trends that contributed to LIBE's position on GDPR are still a critical aspect of LIBE policy making today.

## **PART I: LIBE 1995-2013**

Historically, LIBE has struggled to address the real and perceived attacks on civil liberties that mass data processing by intelligence services can produce. There is no EU capacity to cover standard intelligence service activities.<sup>[14]</sup> As such, the work of national intelligence services is well beyond the control of the European Parliament (EP),<sup>[15]</sup> and certainly beyond the capacity of LIBE.<sup>[16]</sup> The GDPR in its final form does not interfere with the processing of data for national security purposes, as member states can introduce derogations where the transfer of private data to third countries is necessary for reasons of public interest, including national security and the prevention and detection of crime amongst others.<sup>[17]</sup> However, historical limitation on the national security competencies of the EU have not prevented significant parliamentary scrutiny of the work of national intelligence services in the EU and in the US.

A key example of this engagement is the EP's involvement in the Echelon Affair from 1998-2002. The Echelon network system intercepted private and economic communications, developed and managed by the Five Eyes intelligence alliance.<sup>[18],[19]</sup> Though the EP eventually set up a temporary committee explicitly for the investigation of the Echelon network,<sup>[20]</sup> LIBE critically re-launched debates in Parliament in 2000 during a "hearing on the European Union and data protection, during which the second text on Echelon was presented, the existence of Echelon having by then been confirmed by American sources."<sup>[21]</sup>

This early connection between data protection and the activities of intelligence services continued as LIBE, and the EU,<sup>[22]</sup> developed in the years following 2002. The Treaty of Lisbon increased the power of the EP in the EU legislative process.<sup>[23],[24]</sup> Still, prior to the Treaty of Lisbon, the operation of EP committees mattered because "most of the discussions [framing the legislation took] place at the committee level, making the leading committee largely responsible for examining the details of the proposal and starting negotiations with the Council and the Commission."<sup>[25]</sup> In many ways committees are "the central bodies of the institutions,<sup>[26]</sup> determining the behavior of their members as well as the policy outcomes."<sup>[27]</sup> In this context, LIBE rapporteurs<sup>[28]</sup> often criticized attempts to moderate policy proposals for data protection from the Commission as adjusting to "the lowest possible common denominator"<sup>[29]</sup> and repeatedly called for the introduction of a more extensive data protection framework.<sup>[30]</sup>

The SWIFT affair began in June 2006 and reinforced LIBE's focus on data protection. European and US media had published the existence of the Terrorist Finance Tracking Program (TFTP), established by the U.S. Administration, which "allow[ed] US authorities to access all the financial data stored by SWIFT (Society for Worldwide Interbank Financial Telecommunications)."<sup>[31]</sup> The EP adopted a resolution in July 2006, "requiring in particular that the Committee on Civil Liberties, Justice and Home Affairs (LIBE) together with the Committee on Economic and Monetary Affairs (ECON) hold a joint hearing with the private and public parties involved in the affair in order to ascertain what information they may have had."<sup>[32]</sup> Debates on the SWIFT dossier extended through 2010. When an agreement finally entered into force on February 1, 2010, it required a vote from LIBE. LIBE, exercising the EP's new powers to influence the conclusion of international agreements, established by the Treaty of Lisbon,<sup>[33]</sup> rejected the agreement. The U.S. rapidly adjusted, inviting "key MEPs, led by the rapporteur and the LIBE committee's chairman, to visit the US."<sup>[34]</sup>

In September 2011, LIBE had a study completed on "Parliamentary Oversight of Security and Intelligence Agencies in the European Union."<sup>[35]</sup> The study noted that "over the past decade, the EP has developed a growing interest in national security agencies."<sup>[36]</sup> Evidence for this included "strong interest in the development of the new regulation on Frontex, the Europol and Eurojust decisions, as well as two temporary committees that examined the activities of national security agencies and made important recommendations in regard to oversight."<sup>[37]</sup>

Though LIBE began to truly exercise power on the international stage in the 2000s, the EU has an established history of dealing with data protection, dating back to the Data Protection Directive of 1995.<sup>[38]</sup> In January 2012, the Commission of the European Union released a Proposed Data Protection Regulation, designed, as all EU regulations are,<sup>[39]</sup> to be directly binding on member states.<sup>[40]</sup> The LIBE committee subsequently began to formulate the EP's amendments to the General Data Protection Regulation proposal,<sup>[41]</sup> and on April 12, 2012 LIBE appointed committee member Jan Philipp Albrecht as official rapporteur of the European Parliament for GDPR.<sup>[42]</sup>

In October 2012, a briefing note produced on Cloud Computing for the LIBE Committee highlighted the loopholes of the U.S. Foreign Intelligence Surveillance Act (FISA),<sup>[43]</sup> and their consequences for EU citizens' rights and protection.<sup>[44]</sup> LIBE held a hearing for the presentation of the briefing note to the entirety of the European Parliament, following a session on the EU Cybersecurity strategy on February 20, 2013, and asking for "immediate proposals to meet the LIBE amendment deadline on the Data Protection Regulation."<sup>[45]</sup> Yet by March, "the level of interest in the note declined, and there seemed only a remote possibility that Parliament would support fundamental revisions of the Data Protection Regulation."<sup>[46]</sup>

In the months following June 2013, LIBE received approximately 4,000 potential amendments submitted by separate parliamentary committees. Such a dramatic shift in interest suggests that the watershed moment for the progression of GDPR is significantly attributable to NSA contractor Edward Snowden.

## **PART II: LIBE JUNE 2013 – OCTOBER 2013**

On June 5, 2013, Glenn Greenwald published the first of Edward Snowden's disclosures in *The Guardian*.<sup>[47]</sup> A Resolution of the European Parliament on July 4, 2013 gave LIBE a broad mandate "to engage in fact-finding concerning Snowden's disclosures, and to assess their impact on the fundamental rights of EU citizens."<sup>[48]</sup> Claude Moraes, appointed the rapporteur for the inquiry, produced the concluding "Moraes Report."<sup>[49]</sup> A year later, in July 2014, Moraes was elected Chairman of LIBE.<sup>[50]</sup> Then, in November 2014 while giving a lecture at the London School of Economics, Moraes said: "The next phase of our enquiry has to be on where we take this concept of privacy, where we take the concept of regulation. It is an extremely challenging time... I don't have huge faith in many member states to do this, there's so many vested interests, vested security interests to not do this – but we have to try and do this."<sup>[51]</sup>

LIBE called for an inquiry, and hearings began in September 2013. These hearings saw "public questioning of a number of important stakeholders in the issue area, including privacy officers, (former) security services staff, EU Commission officials, and IT specialists."<sup>[52]</sup> Notably absent from these hearings were "those national European security agencies believed to be cooperating with the NSA."<sup>[53]</sup>

LIBE also requested formal studies following the Snowden leaks, the first of which was completed in September 2013, paralleling the hearings. Titled “The US Surveillance Programs and Their Impact on EU Citizens’ Fundamental Rights,” the study explored “the scope of surveillance that can be carried out under the 2008 Amendments Act of US Foreign Intelligence Surveillance (FISA) and related practices of US authorities, which have very strong implications for EU data sovereignty and the protection of European citizens’ rights.”<sup>[54]</sup>

In October 2013, LIBE drew further correlations between data protection and the operation of security services. This is largely evidenced by another study for the committee titled “National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law.”<sup>[55]</sup> The study concluded that “intelligence communities’ understandings and practices of national security and member states’ surveillance programmes jeopardize the EU principle of ‘sincere cooperation,’ as they make it more difficult to carry about the tasks following the Treaties.”<sup>[56]</sup>

Still, pointed studies were not the only results of the Snowden inquiry. SWIFT representatives testified before LIBE in September 2013 during LIBE’s investigation. On October 16, 2013 the SWIFT Agreement was officially suspended as a direct result of Snowden’s disclosures.<sup>[57]</sup> This suspension gave GDPR rapporteur Jan Philipp Albrecht the opportunity to draft an unofficial joint motion in which he pointed out that: “Although the Parliament has no formal powers to initiate a suspension or termination of an international agreement, the Commission will have to act if Parliament withdraws its support for a particular agreement.”<sup>[58]</sup> This statement evidences the willingness of LIBE members to find means of pursuing policy agendas despite having comparatively little formal capacity to do so.

The controversy around the revelations of the various NSA programs apparently made an impression on MEP Albrecht. In 2015 Albrecht wrote that “the revelation by Edward Snowden regarding the mass storage and analysis of details relating to our everyday lives by the secret services and their agents within the internet companies only served to demonstrate to us all how far things have already developed and how little regulation or effective control the people and society are able to muster.”<sup>[59]</sup> Albrecht later became the rapporteur for the EU Police Directive,<sup>[60]</sup> relating to the processing of personal data by competent authorities “for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.”<sup>[61]</sup>

During the inquiry on October 21, 2013, LIBE voted to adopt the compromise draft for the GDPR. This draft significantly increased potential sanctions for non-compliance, extended the territorial scope of the regulation, reviewed third country data transfers, placed limits on profiling, and introducing new requirements for Data Protection Officers.<sup>[62]</sup> The compromise draft passed with an impressive majority, with 49 of LIBE members voting in support, one against, and three abstentions.<sup>[63]</sup> Importantly, the territorial scope expanded at this stage to include those companies operating in the EU with European citizen customers, introducing the extra-territorial reach of the legislation that survived to the finalized version of GDPR of 2016.<sup>[64]</sup>



This vote represented a significant step in more than two years of discussions and lobbying leading to a plenary legislative resolution on March 12, 2014.<sup>[65]</sup> Debates in this period took place during the EP's first reading of the legislation.<sup>[66]</sup> The Council of the European Union agreed on its first reading position on the GDPR in June 15, 2015. The ensuing stages further evidence the LIBE committee's efforts to discuss the processing of personal data for national security matters in concert with the data protection standards required of private corporations.

### **PART III: LIBE OCTOBER 2013–JANUARY 2017**

The importance of data privacy and data protection became increasingly apparent in the public space after 2013. Three instances of LIBE's legislative activities will be used as a lens to evaluate the continuing efforts of LIBE to manage the tenuous relationship it found between security and privacy: the 'anti-FISA' clause of GDPR, the Police Directive, and the ePrivacy Regulation.

After passing the first reading of the EP in 2014, GDPR negotiations progressed to negotiations involving representatives from the EP and the Council of the European Union. Due to LIBE's responsibility for GDPR, their representatives were the primary negotiating team for the EP.<sup>[67]</sup> By September 2015, Article 43a – nicknamed 'the anti-FISA'<sup>[68]</sup> – remained a problem.<sup>[69]</sup> The clause mandated that EU companies should not have to supply Europeans' personal data to non-European countries. It caused broad industry concern, and a letter to legislators from the European Data Coalition explained that Article 43a "unilaterally assum[ed] universal jurisdiction...put[ting] European companies in an unsolvable dilemma and would be in conflict with the concept of interoperability that, while recognizing different privacy concepts, is necessary in international data flows."<sup>[70]</sup>

Coalition appeals did little to change the mind of legislators. The Industry Coalition for Data Protection (ICDP), which represented companies such as Apple and Google, also sent letters to the top regulation negotiators, including the parliamentary GDPR rapporteur Jan Philipp Albrecht. ICDP argued that Article 43a deliberately created legal conflicts and undermined "both the principles of reciprocity in diplomatic relations as well as the credibility of EU data protection reform."<sup>[71]</sup> Still, Article 43a came into force as Article 48<sup>[72]</sup> on "Transfers or disclosures not authorized by Union Law"<sup>[73]</sup> in the final draft of GDPR.<sup>[74]</sup>

More broadly, GDPR can be considered in the context of the EU Protection Data Reform Package, a reference to the combined development of GDPR and its significantly less well-known companion, the Police and Criminal Justice Authorities Directive.<sup>[75]</sup> The EU passed both of pieces of legislation in May 2016; they became applicable to member states in May 2018. Notably, prior to the Police Directive, scholars critiqued data protection in the sector of law enforcement and criminal justice for "offering no stable or uniform legal structure and causing considerable legal uncertainty and inconsistent enforcement of data protection rules."<sup>[76]</sup>

However, whatever regulation exists in the context of police forces and criminal justice is intrinsically related to the activities of member state security services. Indeed, “There is a close cooperation between law enforcement authorities and intelligence services,” as “in the prevention and investigation of crime, these bodies often exchange intelligence with each other.”<sup>[77]</sup> The LIBE-commissioned studies of 2013 used this closeness to justify potential future efforts by LIBE to extend its competencies to the regulation of the activities of member state intelligence services. Justification for this potential extension of EU power pointed to the already present potential spillover of intelligence services activities “into the activities and responsibilities of EU agencies.”<sup>[78]</sup> As such interactions were already taking place, it followed that the EU might have an implied competence to regulate the activities of member state intelligence services.

The actual impact of the Police Directive on the operation of security services is not entirely clear. The Directive does represent the first time that “data protection in the...area of police and judicial cooperation in criminal matters shall be covered by a single legal instrument with direct effect in national legal systems.”<sup>[79]</sup> When compared to GDPR, though, “the final version of the Directive still maintains a number of vague provisions open to interpretations and at times establish[es] low or inadequate data protection standards.”<sup>[80]</sup> The dichotomy of a robust GDPR and a weak Police Directive when LIBE had the primary responsibility for both pieces of legislation suggests that LIBE’s final aim of managing the data processing capability of security services has yet to be realized.

Though GDPR and the Police Directive are in force, the EU and LIBE are continuing to legislate on data protection. The question of LIBE’s perception of the adequacy of current legislation may be evaluated via future developments of the ePrivacy Regulation.<sup>[81]</sup> In January 2017 the European Commission tabled a proposal for a regulation on privacy and electronic communications, which would replace the current 2002 e-Privacy Directive if it became law.<sup>[82]</sup> Once again, LIBE shaped the EP’s amendments to the European Commission proposal.

The ePrivacy Regulation focuses on the security of online communications. It remained bogged down in debates at the time of writing.<sup>[83]</sup> However, the draft the EP approved in May 2018 required “Skype, WhatsApp, iMessage, video games with player messaging and other electronic services that allow private interactions to obtain people’s explicit permission before placing tracking codes on users’ devices or collecting data about their communications.”<sup>[84]</sup> Once again, Jan Philipp Albrecht shepherded the legislation through the EP.<sup>[85]</sup> Trade groups and tech companies “have waged a furious, multipronged lobbying campaign to shut down, or at least weaken, the legislation.”<sup>[86]</sup> These efforts include sponsoring studies that are rife with dire economic predictions of the ePrivacy Regulation’s impact on business opportunities for years to come.<sup>[87]</sup>

## CONCLUSION

LIBE is in a difficult legal position. Privacy and data protection are fundamental rights affirmed by EU primary and secondary law.<sup>[88]</sup> Concurrently, the intersection of individual privacy rights and national security requirements is nuanced and complicated territory. LIBE's mandate requires that it take responsibility for legislation that pertains to data privacy and protection.<sup>[89]</sup> However, when such a position of power is abused, and the complexities of the issues LIBE must address are oversimplified, the potential exists for significant and serious consequences. LIBE continues to frame the US as an unreliable partner for data protection, as evidenced by LIBE's recent resolution to suspend the data exchange deal arranged by the EU-US Privacy Shield, with LIBE Committee Chair and rapporteur Claude Moraes saying "Privacy Shield in its current form does not provide the adequate level of protection required by EU data protection law and the EU Charter."<sup>[90]</sup> The same resolution that suspended Privacy Shield expressed LIBE concerns regarding the US adoption of the CLOUD Act, "which expands the abilities of American and foreign law enforcement to target and access people's data across international borders without making use of the instrument[s]...which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located."<sup>[91]</sup> Similarly, the resolution also voiced concern on "those issues related to national security, such as the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA)."<sup>[92]</sup> Clearly, the LIBE committee maintains that individual data privacy has been unduly sacrificed for expansive national security aims.

Due to GDPR's current presentation as a model for other countries aiming to develop their own data privacy protection frameworks, this paper's approach allows for a more nuanced view of the political climate in which LIBE operates and GDPR exists. As technological advancements in data processing and analysis create new vulnerabilities and opportunities for both public and private sector entities, it is essential to critically evaluate not only the regulatory standards that exist but also the opinions that inform them. 🛡️

## NOTES

1. Deb Reichmann, "U.S. Expects Fallout From Snowden Leaks for Years to Come," *U.S. News*, June 3, 2018, <https://www.usnews.com/news/world/articles/2018-06-03/5-years-on-us-government-still-counting-snowden-leak-costs>.
2. *Ibid.*
3. Hereafter referenced as "LIBE" or "the LIBE Committee."
4. Tracy Connor, "Spy Chief Clapper: We've been snooping on our friends for years," *NBC News*, October 30, 2013, <https://www.nbcnews.com/news/us-news/spy-chief-clapper-weve-been-snooping-our-friends-years-flna8C11488415>.
5. *Ibid.*
6. The LIBE Committee holds responsibility in the European Parliament for "the establishment and development of an area of freedom, security and justice while respecting the principles of subsidiarity and proportionality, in particular: (a) measures concerning the entry and movement of persons, asylum and migration, (b) measures concerning an integrated management of the common borders, (c) measures relating to police and judicial cooperation in criminal matters, including terrorism, and substantive and procedural measures relating to the development for a more coherent Union approach to law; (5) the European Monitoring Center for Drugs and Drug Addiction the European Union Agency for Fundamental Rights, Europol, Eurojust, Cepol, the European Public Prosecutors Office, and other bodies and agencies in the same area..." European Parliament. *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, [http://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf).
7. The LIBE Committee holds responsibility in the European Parliament for "the establishment and development of an area of freedom, security and justice while respecting the principles of subsidiarity and proportionality, in particular: (a) measures concerning the entry and movement of persons, asylum and migration, (b) measures concerning an integrated management of the common borders, (c) measures relating to police and judicial cooperation in criminal matters, including terrorism, and substantive and procedural measures relating to the development for a more coherent Union approach to law; (5) the European Monitoring Center for Drugs and Drug Addiction the European Union Agency for Fundamental Rights, Europol, Eurojust, Cepol, the European Public Prosecutors Office, and other bodies and agencies in the same area..." European Parliament. *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, [http://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf).
8. Scholarship completed as recently as 2017 and 2018 have begun to include important references to the activities of LIBE. (Valentin Gros, Marieke de Goede, Beste Îsleyen. "The Snowden Files Made Public: A Material Politics of Contesting Surveillance." *International Political Sociology* 11, no. 1 (March 2017): 73-89, and Laima Jančiūtė, "EU Politics and the Making of the General Data Protection Regulation: Consolidation, Policy Networks, and Institutionalism in the Process of Balancing Actor Interests." PhD diss., University of Westminster, 2018.
9. Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, 1-88. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679>.
10. Knud Erik Jørgensen, "Introduction: Theorizing European Foreign Policy." In *The SAGE Handbook of European Foreign Policy*, edited by Knud Erik Jørgensen, Aasne Kalland Aarstad, Edith Driessens, Katie Laatikainen, and Ben Tonra, 77, Los Angeles, London, New Delhi, Singapore, Washington D.C., Boston: SAGE Publications, 2015.
11. *Ibid.* 90, References made to A. Niemann (2006) *Explaining Decisions in the European Union*. Cambridge: Cambridge University Press, and P.C. Schmitter (1969) "Three neo-functional Hypotheses about International Integration," *International Organization*, 23(1), 161-166.
12. *Ibid.*, 90.
13. *Ibid.*, 90.
14. "This is affirmed by the treaties that govern the European Union, as "according to Article 4(2) TEU and Article 72 TFEU, data process for 'national security purposes fall outside the scope of the EU laws." (Cristina Blasi Casagran, "Data safeguards for the intelligence collected and shared by Member States." In *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, 164-207. London, UK: Routledge, 2016.) There is also no explicit definition of the term "national security" in the EU laws, so the exception it provides for may be interpreted to the full extent of its potential ability to prevent EU encroachment on the sovereign powers of Member States, Casagran, "Data safeguards for the intelligence collected and shared by Member States," 165.

## NOTES

15. Hereinafter referenced as the “EP.”
16. The caveat to this is that the EU can sometimes play a coordinating role in national security issues as demonstrated by the Schengen Information System. “Instead, the regulation of national security issues falls under the exclusive competence of the member states. The EU’s role in this area would be purely co-ordinative, if any. For instance, one of the few examples of this limited EU role in national security matters is found in the regulation of the Schengen Information System,” Casagran, “Data safeguards for the intelligence collected and shared by Member States,” 167.
17. European Data Protection Board. “Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679.” Adopted on May 25, 2018. [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf).
18. The Five Eyes member states are Australia, Canada, New Zealand, the United Kingdom, and the US.
19. Franco Piodi and Mombelli Iolanda, *The ECHELON Affair: The EP and the Global Interception System 1998-2002*. Study. PE 538.877. Brussels: Directorate-General for Parliamentary Research Services, Historical Archives Unit, 4. [http://www.europarl.europa.eu/EPRS/EPRS\\_STUDY\\_538877\\_AffaireEchelon-EN.pdf](http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf).
20. “At its meeting of 13 April 2000, the Conference of Presidents rejected the proposal to set up a committee of inquiry and approved the creation of a temporary committee: a decision was taken accordingly on 15 June. Both decisions by the Conference of Presidents – rejection of a committee of inquiry and the setting up of the temporary committee – were approved by Parliament on 5 July 2000,” Ibid 19.
21. Ibid 13.
22. Hereinafter referenced as the “EU.”
23. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, December 13, 2007. *OJ C 306, 17.12.2007*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A12007L%2FTXT>.
24. Today, the ordinary legislative procedure applicable to over 80 policy areas which essentially makes the European Parliament the co-legislating body with the Council of the European Union. Before the co-decision procedure was established the European Parliament had significantly less capacity to influence the development of EU legislation.
25. Further, “Even in those cases where it is only consulted, the EP casts a vote on a committee report rather than on the Commission’s proposal.” Ariadna Ripoll Servent, “Playing the Co-Decision Game? Rules’ Changes and Institutional Adaptation at the LIBE Committee.” *Journal of European Integration* 34, no. 1 (2012): 58.
26. Ibid. 58.
27. Ibid. 58.
28. Since the Treaty of Lisbon, the role of rapporteurs in the EP’s legislative process has undergone significant shifts. An increase in informal negotiations between the EP and the Council of the European Union led to the relative strength of rapporteurs in comparison to committee chairmen, as rapporteurs were often “in a better position to access and steer negotiations, thanks to their direct access to information.” Ariadna Ripoll Servent, “Playing the Co-Decision Game? Rules’ Changes and Institutional Adaptation at the LIBE Committee,” 60.
29. European Parliament. 2008, Report of July 23, 2008 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, A6-0322/2008. Ariadna Ripoll Servent, “Playing the Co-Decision Game? Rules’ Changes and Institutional Adaptation at the LIBE Committee,” 66.
30. Ibid. 66.
31. European Parliament. “The Interception of Bank Transfer Data from the SWIFT System by the US Secret Services.” Public Hearing. October 4, 2006, [http://www.europarl.europa.eu/hearings/20061004/libe/programme\\_en.pdf](http://www.europarl.europa.eu/hearings/20061004/libe/programme_en.pdf).
32. Ibid.
33. European Parliament Liaison Office in Ireland. “EP Civil Liberties Committee to vote on EU-US SWIFT Agreement.” Press Release. Dublin: European Union, February 3, 2010. <http://www.europarl.europa.eu/ireland/en/about-us/ep-civil-liberties-committee-to-vote-on-eu-us-swift-agreement>.
34. Hennis-Plasschaert, MEP, interview, March 2010; MEP, interview, July 2010, Referenced in at Ariadna Ripoll. “The role of the European Parliament in international negotiations after Lisbon.” *Journal of European Public Policy* 21, no. 4 (2014), 568-586. <https://www.tandfonline.com/doi/pdf/10.1080/13501763.2014.886614>
35. European Parliament, 2011, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*. Policy Department C: Citizens’ Rights and Constitutional Affairs, accessed at <https://fas.org/irp/eprint/europarl.pdf>.

NOTES

36. Ibid.
37. Ibid.
38. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281, 23.11.1995, 31–50, <https://eur-lex.europa.eu/eli/dir/1995/46/oj>.
39. In the EU, a “regulation” is a binding legislative act that must be applied in its entirety across the EU. For more information on the variations in EU legislation see: [https://europa.eu/european-union/eu-law/legal-acts\\_en](https://europa.eu/european-union/eu-law/legal-acts_en)
40. The Directive had left room for several remaining differences between national laws for data protection, Paul M. Schwartz, “Information Privacy in the Cloud,” *University of Pennsylvania Law Review* 161, no. 6 (2013), 1639.
41. Wilhelm, Ernst-Oliver. “A Brief History of the General Data Protection Regulation.” *International Association of Privacy Professionals*, last update 2016, <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>.
42. Ibid.
43. Section 702 of Title VII of the Foreign Intelligence Surveillance Act (FISA) “authorizes surveillance directed at non-US persons located overseas who are of foreign intelligence importance,” James R. Clapper, and Eric H. Holder, Jr., “Letter re Title VII of the Foreign Intelligence Surveillance Act (FISA).” February 8, 2012, <https://www.justice.gov/sites/default/files/ola/legacy/2012/11/08/02-08-12-fisa-reauthorization.pdf>.
44. European Parliament. *Fighting Cyber Crime and Protecting Privacy in the Cloud*. Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, and Amandine Scherrer, PE 462.509, Brussels: Parliament Department C: Citizens Rights and Constitutional Affairs, 2012, [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE\\_ET\(2012\)462509\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf).
45. In 2012 the LIBE committee commissioned a briefing Note on “Fighting Cybercrime and Protecting Privacy in the Cloud” from the Center for European Policy Studies (CEPS) and the Centre d’Etudes Sur les Conflicts, Liberté et Sécurité (CCLS). “Sections of the Note clearly asserted that Cloud computing and related US regulations presented an unprecedented threat to EU data sovereignty.” (European Commission, “LIBE Committee Vote Backs New EU Data Protection Rules,” Press Release, MEMO-13-923, October 22, 2013, [http://europa.eu/rapid/press-release\\_MEMO-13-923\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-923_en.htm).) The Note included the February 2013 observation that “So far, almost all the attention on [conflicts of international public law] has been focused on the US PATRIOT ACT, but there has been virtually no discussion of the implications of the US Foreign Intelligence Surveillance Amendment Act of 2008. Section 1881a of FAA for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to Cloud computing” European Parliament. *Fighting Cyber Crime and Protecting Privacy in the Cloud*. Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, and Amandine Scherrer, PE 462.509. Brussels: Parliament Department C: Citizens Rights and Constitutional Affairs, 2012, 35, [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE\\_ET\(2012\)462509\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf).
46. Ibid. 35.
47. Glenn Greenwald, “Verizon Order: NSA Collecting Phone Records of Millions of Americans Daily.” *The Guardian*, June 5, 2013, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
48. European Parliament, *Resolution on the US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens’ Privacy*. Joint Motion for a Resolution. RC-B7-0336/2013. Brussels: European Union, July 2, 2013, <http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN>.
49. The report was officially titled “LIBE (JHA) Committee Inquiry on Electronic Mass Surveillance of EU citizens,” Claude Moraes, “Claude Moraes MEP for London Rapporteur of the LIBE Committee Report on Electronic Mass Surveillance of EU Citizens in the European Parliament,” Claude Moraes, July 26, 2013, <http://www.claudemoraes.com/news/95/25/Claude-Moraes-MEP-for-London-Rapporteur-of-the-LIBE-Committee-Report-on-Electronic-Mass-Surveillance-of-EU-citizens-in-the-European-Parliament>.
50. European Parliament, “Claude Moraes,” MEPs, accessed on August 11, 2018, [http://www.europarl.europa.eu/meps/en/4519/CLAUDE\\_MORAES\\_home.html](http://www.europarl.europa.eu/meps/en/4519/CLAUDE_MORAES_home.html).
51. Natasha Lomas, “Digital Privacy is ‘The New Frontier of Human Rights,’” *Tech Crunch*, November 23, 2014, <https://techcrunch.com/2014/11/23/privacy-human-rights-frontier/>.
52. Valentina Gros, Marieke de Goede, Beste Ísleyen, “The Snowden Files Made Public: A Material Politics of Contesting Surveillance,” *International Political Sociology* 11, no. 1 (March 2017), 74.



## NOTES

53. Ibid. 74.
54. European Parliament, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*. Caspar Bowden and Didier Bigo, Note. PE 474.405. Brussels: Policy Department C: Citizens' Rights and Constitutional Affairs, September 16, 2013, [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/briefingnote\\_/briefingnote\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf).
55. European Parliament, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer. Study. PE 493.032. Brussels: Policy Department C: Citizens' Rights and Constitutional Affairs, October 14, 2013, [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE\\_ET%282013%29493032\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf).
56. Ibid.
57. The Greens in the European Parliament, "Suspension of the SWIFT agreement as a result of NSA Surveillance," October 16, 2013, <https://www.greens-efa.eu/en/article/suspension-of-the-swift-agreement-as-a-result-of-nsa-surveillance/>.
58. European Parliament, *Joint Motion for a Resolution on the Suspension of the TFTP agreement as a result of NSA surveillance*, Joint Motion for a Resolution, RC-B7-0468/2013, Brussels: European Union, October 21, 2013. <http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN>. Referenced in Cristina Blasi Casagran, "Data safeguards for the intelligence collected and shared by Member States," in *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, 184. London, UK: Routledge, 2016.
59. Jan Philipp Albrecht, "Hands off our data!" *Knaur Taschenbuch*, 41, last modified 2015, [https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP\\_Albrecht\\_hands-off\\_final\\_WEB.pdf](https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf).
60. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, 89–131, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0089.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG)
61. Ibid.
62. Hogan Lovells, "EU draft Data Protection Regulation: the LIBE Committee Amendments," Briefing Paper, 1. 2013, accessed August 11, 2018, <https://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf>.
63. European Commission, "LIBE Committee Vote Backs New EU Data Protection Rules," Press Release, MEMO-13-923, October 22, 2013, [http://europa.eu/rapid/press-release\\_MEMO-13-923\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-923_en.htm).
64. According to Article 3 Sections 1 and 2 of the GDPR, the regulation applies if "If the processing of personal data takes place in the context of the activities of an establishment or organization in the EU, regardless of whether the processing itself takes place in the EU (Article 3, Section 1 of the GDPR)," and "If the personal data of individuals who are in the EU is processed by an organization not established in the EU and the processing concerns the offering of goods or services to individuals in the EU, or monitoring the behavior of individuals that takes place in the EU (Article 3, Section 2 of the GDPR)," Matthias Artzt, "Territorial scope of the GDPR from a US perspective," *International Association of Privacy Professionals*, June 26, 2018, <https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/>.
65. European Parliament, "First reading of the European Parliament: European Parliament legislative resolution of March 12, 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading)," A7-0402/2013, Strasbourg: European Union, March 12, 2014, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN>. Referenced Eleni Kosta and Kees Stuurman, "The Draft General Data Protection Regulation," in *The Law, Economics and Politics of International Standardization*, edited by Panagiotis Delimatsis, 441, Cambridge: Cambridge University Press, 2015.
66. For a short review of the EU's Ordinary Legislative Process visit: [http://www.europarl.europa.eu/external/html/legislativeprocedure/default\\_en.htm](http://www.europarl.europa.eu/external/html/legislativeprocedure/default_en.htm)

## NOTES

67. In the case of the GDPR negotiations “The Parliament [was] represented by Jan Albrecht, the rapporteur on the legal text, Claude Moraes, the chairperson of the lead Parliament committee (LIBE committee), shadow rapporteurs, political group coordinators and various staff members of the Parliament.” For a useful synopsis of the ‘trilogue’ negotiations process visit: <https://privacylawblog.fieldfisher.com/2015/unravelling-the-mysteries-of-the-gdpr-trilogues>
68. Neil Ford, “European Data Coalition lobbies against GDPR Article 43a – the ‘anti-FISA’ Clause.” IT Governance, September 3, 2015, <https://www.itgovernance.eu/blog/en/european-data-coalition-lobbies-against-gdpr-article-43a-the-anti-fisa-clause>.
69. Ibid.
70. European Data Coalition, “Re: International data transfers,” August 24, 2015, accessed at: <http://europeandatacoalition.eu/wp-content/uploads/2015/06/Coalition-reaction-on-Ch-V3.pdf>.
71. David Meyer, “Industry issues plea over data reform,” Politico, January 28, 2018, <https://www.politico.eu/article/industry-plea-data-reform-protection-privacy/>.
72. “The GDPR maintains existing restrictions on the transfers of personal data from the EU to third countries or international organizations. These restrictions are aimed at ensuring that the GDPR’s provisions cannot be circumvented by transferring personal data from the EU to a non-EU country with less restrictive data-privacy laws. Pursuant to Article 46, such transfers may only be made to countries that also have adequate data-protection requirements. However, Article 49 of the GDPR also gives member states flexibility to allow the transfer of personal data to third countries absent an adequacy determination if such transfer is “necessary for important reasons of public interest”—for example, if there is a need to transfer health data to a third country in order to deal with an international public-health emergency,” Ali Cooper-Ponte, “GDPR Derogations, ePrivacy, and the Evolving European Privacy Landscape,” *The Lawfare Institute*, last modified May 25, 2018, <https://www.lawfareblog.com/gdpr-derogations-eprivacy-and-evolving-european-privacy-landscape>.
73. “Chapter V (Articles 44 through 49) of the GDPR governs cross-border transfers of personal data. Article 45 states the conditions for transfers with an adequacy decision; Article 46 sets forth the conditions for transfers by way of appropriate safeguards in the absence of an adequacy decision; Article 47 sets the conditions for transfers by way of binding corporate rules; Article 48 addresses situations in which a foreign tribunal or administrative body has ordered transfer not otherwise permitted by the GDPR; and Article 49 states the conditions for derogations for specific situations in the absence of an adequacy decision or appropriate safeguards,” Meyers, “Industry issues plea over data reform,” 2018.
74. Parliament and Council Regulation (EU) 2016/679 of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, 1–88, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679>.
75. European Commission. “Questions and Answers – Data Protection Reform Package.” Press Release. MEMO-17-1441, May 24, 2017, [http://europa.eu/rapid/press-release\\_MEMO-17-1441\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm), hereinafter “the Directive.”
76. Hielke Hijmans and Alfonso Scirocco, “Shortcomings in EU data protection in the third and the Second Pillars. Can the Lisbon Treaty be expected to help?” *Common Market Law Review* 46, (2009): 1496. Referenced in Thomas Marquenie, “The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework,” *Computer Law & Security Review* 33, no. 3 (2017): 325, <https://www.sciencedirect.com/science/article/pii/S0267364917300742>.
77. Casagran, “Introduction,” 5.
78. Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, and Amandine Scherrer, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*. Brussels: Center for European Policy Studies, November 6, 2013, <https://www.ceps.eu/publications/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law>.
79. Marquenie, “The Police and Criminal Justice Authorities Directive,” 338.
80. Ibid. 338.
81. European Commission, “Proposal for a Regulation of the European Parliament and of the Council Concerning the Request for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications),” Brussels, October 1, 2017, [http://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/com/2017/0010/COM\\_COM\(2017\)0010\\_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2017/0010/COM_COM(2017)0010_EN.pdf).
82. Ibid.



## NOTES

83. Reed Smith LLP, “ePrivacy regulation will likely not apply before 2021,” *Lexology*, January 28, 2019, <https://www.lexology.com/library/detail.aspx?g=23653861-8a4e-4cff-9550-717594099922>.
84. Natasha Singer, “The Next Privacy Battle in Europe is Over This New Law,” *NYTimes*, May 27, 2018, <https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html>.
85. *Ibid.*
86. *Ibid.*
87. Anja Lambrecht, *Measuring the Cost of Europe’s E-Privacy Regulation*, Center for European Policy Studies, December 2017, <https://www.ceps.eu/sites/default/files/Executive%20Summary%20-%20E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments....pdf>.
88. This is reinforced by multiple legal documents, including Article 7 of the Charter of Fundamental Rights (CFR), and Article 8 of the European Convention on Human Rights, which also enshrines the right to privacy. Article 16 of the Treaty on the Functioning of the EU (TFEU) frames “the protection of natural persons in relation to the processing of their personal data [as a] fundamental right,” Treaty of Lisbon, 2007.
89. European Parliament, *Rules of Procedure of the European Parliament (2018)*. XVII. Committee on Civil Liberties, Justice and Home Affairs, Brussels: European Union, July 2018, <http://www.europarl.europa.eu/sides/getLastRules.do?language=en&reference=RESP-LIBE>.
90. European Parliament, “Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs,” REF: 20180628IPR06836, Brussels: European Union, July 5, 2018, <http://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps>.
91. European Parliament, *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, [http://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf).
92. *Ibid.*



# The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence

---

Major (Ret.) Jacob Cox, Ph.D.

Colonel Daniel Bennett, Ph.D.

Colonel (Ret.) Scott Lathrop, Ph.D.

Lieutenant Colonel (Ret.) Chris Walls

Chief Warrant Officer 4 (Ret.) Jason LaClair

Lieutenant Colonel Clint Tracy

Chief Warrant Officer 4 Judy Esquibel

## ABSTRACT

With Electronic Warfare joining the Cyber Branch in October 2018, numerous opportunities and challenges that affect warfighters are surfacing. To capture and consolidate some of these observations, the Electronic Warfare Cyber Convergence (EWC2) workshop, held in conjunction with the 2018 Cyberspace Electromagnetic Activities (CEMA) conference, provided an opportunity for experts from military, government, commercial and academic backgrounds to compare insights, explore friction points, consider deeper issues and note potential research opportunities within the EWC2. In this workshop, participants learned that the convergence of EW and cyberspace operations is only the initial step towards the greater goal of controlling information on the battlefield.

*The contributions of Maj. (Ret.) Jacob Cox, Col. Daniel Bennett, Col. (Ret.) Scott Lathrop, Lt. Col. (Ret.), CW4 (Ret.) Jason LaClair, Lt. Col. Clint Tracy, and CW4 Judy Esquibel are the work of the U.S. Government and are not subject to copyright protection in the United States. Foreign copyrights may apply.*

©2019 The MITRE Corporation. ALL RIGHTS RESERVED

## **I. INTRODUCTION**

On October 1, 2018, the United States Army merged its electronic warfare (EW) functional area into its Cyber Branch. This merger supports the Army's doctrinal requirement to perform cyberspace and EW operations in support of unified land operations and joint operations.<sup>[1]</sup> As with any merger, however, friction points involving culture, policy, doctrine, operations, and technology can create obstacles to achieving a cohesive organization. To address these challenges, the U.S. Army must identify and address the merger's shortfalls across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P). The desire to address these shortfalls was at the forefront of the inaugural Electronic Warfare Cyber Convergence (EWC2) Workshop, which was organized and moderated by the Army Cyber Institute (ACI) and industry volunteers in collaboration with the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S), Communications-Electronics Research, Development and Engineering Center (CERDEC),<sup>[2]</sup> and the Association of Old Crows (AOC).

During the workshop's two-day event, leaders, operators, and researchers across military services, defense agencies, and civilian organizations discussed, debated, and identified friction points, hurdles, and ways forward within the converging EW and Cyber communities. Workshop focus areas included innovative research, training, and opportunities to advance and support CEMA.<sup>[3]</sup> Participants also explored how to leverage this convergence to allow commanders to outmaneuver adversaries, both physically and cognitively, in multi-domain battle. Products of this event included a consolidated set of friction points and challenges facing EW and Cyber convergence along with suggestions and opportunities for enabling friendly forces to operate effectively in the current and future battlefield. Moreover, participants focused on how to seamlessly achieve these goals for warfighters who ultimately care about how cyberspace and EW operations will enable them to gain dominance in multi-domain battle and win.

The topics of this workshop evolved from a discussion of friction points that were created with the convergence of EW and Cyber. The ACI encouraged exploration of operational and personnel gaps; and the link between EW and cyberspace operations and information operations (IO). Technological challenges discussed at TechNet 2018 contributed to the selection of machine learning (ML) and artificial intelligence (AI) as enablers for cyberspace and EW operations. These topics led to the workshop's five focused areas: 1) general friction points of EW/Cyber convergence; 2) employment of EW/Cyber personnel; 3) operational employment of EW/Cyber capabilities; 4) employment of AI/ML in cyberspace and EW operations; and 5) leveraging CEMA for IO. Each participant was assigned two topic areas based on experience, expertise, and interest. Participants rotated between focus areas on both days of the workshop. As a result, the participants generated vibrant discussions on directions, trends, and challenges of EW/Cyber convergence and were challenged to develop questions about gaps, friction points, and research opportunities for each of these topics. These discussions

also led participants to acknowledge that greater convergence is yet to come as more areas of expertise fall under information warfare operations. This report summarizes the workshop's outcomes, which will ideally serve to drive future discussions by leadership and researchers to close gaps, smooth friction points (perceived or not), and pursue research opportunities to improve cyberspace and EW operations.

## II. BACKGROUND

Before convergence, EW and Cyber communities were largely separated and widely varied across the military services in terms of equipment, unit organization, operational tasks, and culture. Meanwhile, near-peer adversaries have demonstrated integrated EW and cyberspace capabilities along with Signals Intelligence (SIGINT) and Information Operations (IO) capabilities in real-world operations. Russia's use of EW/Cyber/SIGINT/IO<sup>[4]</sup> during its conflict with Ukraine, and in Syria, proved particularly illuminating—indicating future conflicts will require kinetic and non-kinetic maneuver, both physically and cognitively, across multiple domains.<sup>[5]</sup> For instance, adversaries may attempt to strike at homeland installations via kinetic and non-kinetic means to disrupt or delay deployment of forces, manipulate national commitment to potential or ongoing conflicts, or disrupt the warfighting functions of deployed units.

We now expect our enemies to employ cyberspace attack capabilities (such as disruptive and destructive malware); EW capabilities (jamming and signal geolocation), and space capabilities that obstruct satellite use to disrupt U.S. military communications; positioning, navigation, and timing (PNT); synchronization; and freedom of maneuver. These threats make it clear—if the U.S. military is to succeed in this future battlespace, it must gain combat superiority over its adversaries by defending its information networks in cyberspace and securing unimpeded access to the electromagnetic spectrum (EMS) while denying its adversaries the ability to do the same.

These concerns are driving the Army to challenge the way it employs personnel, conducts operations and focuses on technological capabilities. In response, the EWC2 workshop provided a collaborative environment for participants to discuss, debate, organize and determine the friction points, hurdles, and ways forward within the converging EW and Cyber communities. During multiple breakout sessions, participants attempted to identify friction points, doctrinal gaps, and innovative research needed to advance and support cyberspace and EW operations. Hence, the workshop's outcomes focused on the next stage of technical and non-technical objectives needed to enable friendly forces to operate effectively in current and future multi-domain battlefields while deterring the adversary's ability to do the same.

## III. GENERAL EW/CYBER FRICTION POINTS

Mergers frequently struggle with a clash of personalities, cultures, priorities, and leadership that creates points of friction or resistance to a unified application of effort. For instance,

during the workshop, one participant expressed concern that there is a potential for the Army's EW/Cyber convergence campaign to erode the fundamental understanding that cyberspace operations and EW operations are at their core separate and distinct capabilities with unique pros and cons. For instance, EW seeks to preserve the EMS for friendly use while denying its use to the enemy. Subdivisions of EW include electronic attack (EA), EW support (ES), and electronic defense (ED)<sup>[6]</sup> Cyberspace operations (CO) include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoD information network (DODIN) operations. Cyberspace operations employ cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace,<sup>[7]</sup> which admittedly depends on the EMS at the physical communication layer. However, these two capabilities have different focuses, requiring different high-demand, low-density skill sets.

By merging EW and cyberspace capabilities, the U.S. Army hopes to achieve better coordination across the EMS and cyberspace to gain advantage over its adversaries. The potential to dilute skills and training resources that are already inherent in EW and cyberspace workforces does exist. In 2016, Senft stated that the convergence of Cyber and EW would further degrade the already limited resources allocated for EW.<sup>[8]</sup> He argued that EW is only used in the continuum of military operations during Phase 2, "Seize the Initiative," while cyberspace capabilities are employed during all phases of military operations causing it to receive more attention and resources. Arguably, EW has a role during other phases, but Senft's point raises a valid concern that resourcing remains an issue across training, equipping, and staffing. Hence, participants asked how the Army can better allocate resources without further constraining EW capabilities?

Participants noted that current friction points mostly reside in the acquisition, policy/authorities, classification boundaries, and force structure. Much work is needed to balance requirements with system acquisition processes to ensure better vendor engagement. Policy/authorities were the most contentious of the friction points listed above. The majority of working group members view policy/authorities as a hindrance to mission accomplishment. However, working group members noted that it is not necessarily policies per se, that are the problem, but rather the interpretation of the policies at the strategic and operational level that falls short. This happens when there is a lack of technical understanding required to accurately and quickly validate a tactical course of action (COA). Maturing of the force and additional training for personnel working at the strategic and operational level will help in this regard. From a classification standpoint, participants expressed frustration at the lack of cross-domain solutions available for sharing operationally relevant data with warfighters. If commanders and staff are to gain the advantage over adversaries in multi-domain battle, the Army must pursue a national-level forcing function to ensure they receive relevant information promptly.

#### IV. EMPLOYMENT OF EW/CYBER PERSONNEL

The Army has taken great strides towards increasing its capability to conduct EW and cyberspace operations. The initial focus was on staff-level manning with the creation of the CEMA sections as the staff focal point for planning, integration, and synchronization of EW and cyberspace operations. These staff elements are expected to be organic at each echelon from the Brigade headquarters to Theater Army, and they are staffed with existing EW and Spectrum Management Officer (SMO) personnel, plus some limited new personnel authorizations. Unfortunately, these members have received limited or no training on their new requirements. Moreover, the lack of EW equipment resulted in limited training on the actual conduct of EW operations. Similar SMO training primarily focuses on the administrative tasks of spectrum planning and deconfliction rather than spectrum maneuver. As a result, a major overhaul of training is required to enable the CEMA section to perform as designed. CEMA Section personnel need to be experts in EW systems with a strong grasp of existing cyberspace capabilities. Additionally, SMO personnel must be trained to advise the CEMA section on the best employment of its assigned capabilities based on the EMS and physical terrain aspects of the operating environment and to help mitigate the unintended effects of employed systems. In addition to individual and collective training at the tactical level, the CEMA section also requires classified intelligence and reach-back support to EW and cyberspace subject matter experts to help it address emerging threats in a rapidly changing environment. This reach-back support would help fill training and expertise gaps and could potentially be offered by future formations such as the recently approved Cyber Warfare Support Battalion (CWSB).

The CEMA section also struggles with limited intelligence support. As the Army grows its EW and cyberspace forces, there has been little or no corresponding growth in the supporting intelligence formations. EW and cyberspace operations require specialized technical and timely intelligence as well as the analysis and characterization of collected signals. There is significant work required to shape future operating environments through detailed intelligence preparation of the battlefield (IPB). IPB to support EW and cyberspace operations requires that the electromagnetic and cyberspace environment be baselined along with capabilities to support situational understanding. Electronic Intelligence (ELINT) surveys are required to identify and characterize signals of interest and develop signatures before a conflict to enable EW systems to rapidly identify and target signal and associated adversary units in the opening phases of future conflicts. Current intelligence forces have already struggled to meet existing intelligence requirements before the surge in EW and cyberspace forces and capabilities. The Army will need to expand its intelligence operations in Phase 0 to gather the necessary intelligence and information to enable emerging EW and cyberspace capabilities. In an era of limited resources and numerous critical gaps across the Army, any increase in intelligence capability has not been a high enough priority to be resourced.

To further exacerbate the lack of intelligence, and due to the cross-domain deficiency discussed in the previous section, CEMA sections struggle to receive and share SIGINT and other highly classified information with other associated intelligence elements. The CEMA section, like the rest of their associated headquarters, operates on SECRET networks while their much-needed intelligence support, such as SIGINT, is resident on TOP SECRET networks. CEMA personnel are not currently mandated to receive the level of clearance necessary to receive and work with this information. To integrate with the Mission Command systems on SIPR, current and future EW systems are only required to operate at the SECRET level, which places policy and technological barriers that degrade the effectiveness of current and future capabilities. The lack of cross-domain solutions further exacerbates the exchange of needed information.

The CEMA Cell of the future may also look different than today. The function may end up absorbed into another staff element such as the fires section or a future information warfare section. Regardless of any potential reorganization, the requirements to understand and integrate EW and cyberspace capabilities into operations will remain. The CEMA Cell of the future will have to overcome current issues with sharing classified intelligence with the CEMA Cell being able to access TOP SECRET information needed to plan, integrate, and synchronize EW and cyberspace effects. A fused picture that integrates not only EW and cyberspace information, but also SIGINT, Space, and IO reflecting the latest information and intelligence, must be available to our planners. This capability may look more like the design for the coming Intelligence Cyberspace Electronic Warfare Space (ICEWS) detachment that is a part of the future Multi-Domain Task Force (MDTF). The Army has already identified requirements to invest in a common operating environment (COE) with its command post computing environment (CPCE) that attempts to address these challenges. However, these programs are only in their nascent stages, and much work and research are needed to bring the analytics and tools to bear that will provide commanders and staff with situational understanding. Future CEMA sections must also be experts in utilizing assigned sensors (EW, Cyberspace, Space, and intelligence), intelligence resources, open source information, and battlefield innovation to see and understand their operating environment and to conduct planning to integrate EW and cyberspace capabilities into every operation to provide targeting options and defend their unit's networks and systems. These capabilities should be the basis of collective training for the CEMA section.

### ***Evolving EW Platoons and Training***

As EW platoons are fielded with equipment and capabilities, it becomes critically important to establish common training standards. Like other specialties, the EW Platoons should have both collective and individual task standards that will allow their leaders to establish training plans and determine their unit's readiness for its wartime mission. Today, units are using their initiative to establish their tasks and standards. These tasks and standards need to be passed to Training and Doctrine Command (TRADOC), so they can be normalized and codified into Army tasks and standards. These tasks and standards should be maintained, with the advice



and consent of Army Cyber Command (ARCYBER) as the operational headquarters for all EW and cyberspace forces in the Army, at the Cyber Center of Excellence, an arm of TRADOC.

The newly approved EW platoons at the Brigade level (EW Company at Corps echelon) will work with sensitive equipment that if used improperly could have adverse effects on U.S. Forces, allies, and non-combatants. To ensure that these capabilities are employed correctly, each of the operators should be certified on their assigned equipment. As the Army begins to operationalize tactical cyberspace operations, these units may receive new capabilities in an ad hoc manner. Platoons should look to the mechanized and armor formations and consider using a Master Gunner who is responsible for certifying each of the soldiers on their assigned equipment. New EW/cyberspace capabilities could then be passed through the Master Gunner who would assume responsibility for training the rest of the operators in the platoon. Hence, the Master Gunner would require extensive training both as a cyberspace operator and EW expert. This role is ideally suited for a warrant officer.

In the EW and Cyberspace mission areas, warrant officers are the technical subject matter experts, and they have a training and development track to enable them to fill this role. This makes the warrant officer a key participant of CEMA sections at all echelons as integral to advising the CEMA chief and the commander on the capability and employment of assigned systems. Despite the recognition of their key role, participants noted that warrant officers were left off the EW Platoon's force design. This gap potentially leaves a critical vulnerability in our forward most units of action.

### ***METs and Readiness***

In the Army, a unit's readiness is directly linked to its mission essential tasks (METs). These tasks are the priority for unit training and are typically tracked by commanders. For EW and cyberspace operations to receive the necessary training support, their associated tasks must be included in (or directly influence) the accomplishment of its MET for maneuver formations from battalion to division level. METs are critical as they affect the Objective Task evaluation of a unit's readiness to accomplish its wartime mission. Without this emphasis, unit's will not assign EW and cyberspace operations training the priority required to match peer adversaries.

Emphasis on the importance of EW and cyberspace training must be top-down and heavily integrated. The U.S. Army's Cyber Directorate in the Army G3/5/7 (Operations, Planning and Training section), DAMO-CY, is responsible for developing the Army EW and cyberspace strategy and is uniquely able to orchestrate the integration of all aspects of the man, train, and equip mission into Army foundational documents that will ultimately drive requirements, resourcing, and prioritization. Guidance from these strategies will be amplified through other foundational Army training documents such as the U.S. Army Forces Command (FORSCOM) Training Guidance. This guidance is published annually and serves as the basis from which all Army units develop their priorities for training. The continued requirement to address CEMA in annual training guidance would influence commanders to increase their priority for EW and cyberspace training.

Army exercises also provide an opportunity to increase training emphasis for EW and cyberspace operations. Combat Training Centers have been used to exercise limited EW and Cyberspace capabilities. Unfortunately, these tasks have not been prioritized as critical tasks. When used, Opposing Force (OPFOR) capabilities have seen limited or constrained use due to concerns that it will degrade the unit's networks or systems to the point that it is prevented from achieving its training objectives. Also, EW and cyberspace topics are rarely—if ever—topics of conversation in the commander's end-of-rotation After Action Reviews (AAR). Instead, it is relegated to other AARs not typically attended by commanders. To increase the visibility and importance of EW and cyberspace in the eyes of commanders, the Division Trainer—who is responsible for shaping a Combat Training Center (CTC) rotation—can state that EW and cyberspace operations will be a primary objective for the rotation, which would ensure the rotational Commander's attention and their inclusion in mid-and end-of-rotation AARs. Broader employment of OPFOR EW and cyberspace capabilities would also demonstrate a more realistic threat picture and would likely serve as an eye-opener to how vulnerable forces are to the EW and cyberspace threat. All of these taken together would be a powerful message on the increased importance of EW and cyberspace operations, especially if the message is tied to maneuver.

Cyber and EW communities have primarily addressed cyberspace and EW operations as technical issues, not operational ones. However, to best address the U.S. military's personnel, equipment, and training challenges, a different perspective is needed. Instead of viewing operations through the lens of cyberspace and EW (or even Intelligence, Mission Command, or Fires), leaders need to consider these capabilities through the lens of the maneuver commander. This viewpoint will enable changes in how the U.S. Army approaches these challenges, and it will allow warfighters to effectively integrate cyberspace and EW capabilities into military operations—helping warfighters visualize, describe, and direct operations in the EMS and cyberspace.<sup>[9]</sup>

### ***Recruiting and Retention***

The emerging technological advances in EW and cyberspace capabilities require a more technically-skilled Soldier. The Army has begun to address this challenge through assessing and adjusting basic test scores to qualify Soldiers for these more technical military occupation skills. One challenge is that the type of individuals that are required to perform these missions are inherently sought after in the public workplace, and their value and job opportunities only increase as they receive advanced training in the service. These facts create challenges for recruiting and retaining these soldiers. Several ideas such as monetary bonuses, advanced schooling, assignment stability, and flexible standards on physical fitness and uniform requirements were discussed. While monetary bonuses can help to recruit initial personnel and early bonuses tied to utilization tours could help keep them longer, it is hard for the military to compete with salaries offered in the corporate workplace.

While flexible standards on physical fitness, uniform, and other military standards may sound good at face value, the opinion of the working group was that anything that undermines the military's discipline and sense of mission, which creates camaraderie within the service would do more harm than good by retaining the wrong type of personnel. Similarly, personnel solely motivated by monetary inducements may not have the right motivations necessary to integrate into Army formations successfully. Working group participants suggested that the best personnel are the ones that share the sense of mission and purpose. Furthermore, benefits that help personnel perform their jobs better, such as longer assignment periods, advanced schooling, and the ability to focus and professionalize in specific mission areas are options worth pursuing. However, this is an area deserving of greater investigation and analysis.

### ***Officer Development***

In the new design for EW platoons, a Career Mission Field (CMF) 17 (Cyberspace Warfare) Second Lieutenant is the platoon leader. EWC2 participants questioned whether newly commissioned officers are the ideal candidate for the role. After all, the EW Platoon is a Brigade, not a company, asset. Are lieutenants expected to possess the technical savvy and operational understanding needed to facilitate the employment of EW capabilities? Like other mission areas, lieutenants will likely be responsible for the leadership and operational employment of their platoons and will lean on their non-commissioned officers (NCO) and a warrant officer (if included in the future force design) for technical advice. These officers will receive the same training as an officer destined for service within the Cyber Mission Forces (CMF), but with additional training of EW.

Participants asked whether these officers would benefit from more diversified career paths that include time leading in tactical as well as operational and strategic units. Officers who serve in tactical roles can serve as ambassadors able to translate the highly technical aspects of EW and cyberspace operations into maneuver language that resonates with battlefield commanders. This position also affects the broader Army's perception of EW and cyberspace forces as platoon leaders will serve as the primary point of contact to U.S. military leaders. An argument can also be made that these officers should be the best of the CMF 17 to assist in the adoption and integration of this emerging capability.

## **V. OPERATIONAL EMPLOYMENT OF EW/CYBER CAPABILITIES**

The operational employment of EW/Cyberspace capabilities touched upon intelligence, doctrine, and understanding of capabilities. These gaps stretch across how warfighters receive cross-domain intelligence, apply cyber/EW capabilities and understand the impact of cyberspace and EW operations on their warfighting functions. For instance, there is a gap in the timeliness in which actionable intelligence is extracted from classified sources and shared with warfighters. Participants identified the need to identify a cross-domain solution that can

expedite this process. Understanding the impact of cyberspace and EW operations was also identified as a key weakness for commanders and staff. With regard to understanding the impacts of cyberspace and EW operations on the battlefield, EWC2 participants observed that leaders from Brigade through Division struggle to obtain an adequate understanding of what tasks EW and cyberspace operations can perform. They also lack information about what tools/assets are arrayed to perform these tasks—both within the Army and the broader Joint force. In the Army’s Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EW CBA), published in 2013, Cyber Situational Awareness [Understanding] was listed as the number one gap within its Functional Needs Assessment (FNA) Gaps with Doctrine Aspects.<sup>[10]</sup> Six years later, our research demonstrates this remains a gap in U.S. Army capabilities.

Participants also identified the lack of tools to create, access, or perform collection and effects in support of cyberspace operations as a gap. This discussion developed along two lines. First, what tools are already developed and available to support tactical (BCT-DIV) cyber? Second, what processes exist (or could be created) to rapidly validate existing open source tools for use?

The Army has embraced events like Cyber Quest and Cyber Blitz to help answer these questions and inform requirements. Major General Morrison (Commanding General, U.S. Army Cyber Center of Excellence and Fort Gordon) said as much when he stated that “Cyber Quest will concentrate on enabling more rapid technology to aid the soldiers.”<sup>[11]</sup> Similarly, Cyber Blitz is an experimentation campaign supporting the U.S. Army with the timely transition of innovative Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technical capabilities.<sup>[12]</sup> However, informing warfighters of the results of these events and getting their feedback may still require further progress. These events fall short of emulating an actual tactical environment and are not funded or resourced except for a fraction of the devices and services found in actual units. These issues represent a clear gap in rapidly validating new tools and getting them into the hands of warfighters. Resourcing also hinders operator led design.

Advantages that the U.S. Army have in cyberspace and EW operations are that Soldiers are resourceful, and they are capable of innovating in the field, yet, some EWC2 participants stated that higher headquarters might be hesitant to allow such innovations without proper validation and certification. What is interesting about these questions is that many EWC2 participants believe that there is a need for some level of cyberspace and EW operations capability to be organic to warfighters at DIV-BCT. This lack of communication or shared vision likely serves as a friction point across the Army’s leadership. Perhaps Army leadership should reevaluate what capabilities, if any, should be passed down to lower echelons and then educate leadership and staff as to why other capabilities are best suited for execution at the Army Service Component Command (ASCC) level (i.e., ARCYBER).

Some working group (WG) participants also stated they believe there is friction with authority as it applies to training and operations. The perception, whether true or not, is that very few leaders, lawyers, and legislators are competent in cyber law, policy and operations. This gap potentially prevents requests from being generated and staffed at BCT-DIV. Because of this observation, workshop attendees asked what mechanisms exist or could be created to tutor senior leaders (COL and above) who are currently in command and staff positions to close their education gaps in cyberspace operations and policy. A similar question included legislators: what mechanisms exist or could be created to tutor legislators to make more informed policy decisions regarding Cyber/EW.

Workshop participants also questioned how many BCT or Special Forces Group (SFG) Judge Advocate General (JAG) officers possess the competency to inform a legal brief describing whether an internally generated cyber training or operations concept is legal? Perhaps a more important question regarding the use of JAG officers is at what point in training/deployment preparations should a JAG officer be integrated into the military decision-making process (MDMP) for CEMA planning and COA development? If achieved, would integrating the JAG officer into the Cyber/EW planning process could also help close individual education gaps of commanders and staff about cyberlaw?

## **VI. EMPLOYMENT OF AI/ML IN EW/CYBER OPERATIONS**

To effectively employ EW and cyberspace operations at “machine speed” in future, multi-domain operations, workshop participants discussed the incorporation of artificial intelligence/machine learning (AI/ML) in future systems. This could help overcome training lapses and hasten the response time of U.S. Forces to respond to EW- and cyberspace-based attacks. The ability for EW and cyberspace systems to autonomously detect, characterize, and respond to signals of interest will be increasingly important to protect against electronic attack, to deny signals, or to manipulate signals for exploitation. During TechNet 2018, Colonel Steven Rehn, TRADOC Capability Manager (TCM) for Cyber at Fort Gordon, GA, offered several areas where AI can aid EW and cyberspace capabilities. For instance, he stated the application of AI could help reduce the time needed for EW and cyberspace systems to reconfigure and change techniques (or tools) to enable and protect friendly forces’ access to EMS and information systems (IS) while denying adversaries access to the same.

During the workshop, participants discussed what AI/ML is, its applicability to cyberspace and EW operations, and some of the challenges that must be addressed. In general, AI is a set of algorithmic approaches for improving the functionality and performance of a computational system. It reduces the workload of system operators, so they can focus on higher-level, cognitive tasks.<sup>[13]</sup> In effect, the underlying software is more intelligent and, reduces the number of low-level tasks that one must perform. For example, a voice recognition system reduces the amount of keyboard input. We can think of AI in terms of three overarching goals.

First, some AI emulates *intelligent behavior*. These systems attempt to act as a human would, regardless of whether the underlying sensing or computations are human-like. Driverless cars are a good example: the goal is to have these cars drive like a human would, or perhaps even better. Many times, little regard is given to the corresponding human analogy of the underlying sensors (e.g., LIDAR vs. eyes) and computations (e.g., search algorithm vs. visual-spatial reasoning). A second goal is the emulation of *intelligent thinking*. For example, Amazon's Alexa and Google's Home receive human voice as an input, perceive the verbal question through an ML model, encode it into an internal knowledge representation, decide on an answer through knowledge search, and then encode and deliver an audio response. Finally, some AI goals are to surpass *human performance*. State of the art image recognition systems are now equaling, or in some cases, superseding human performance. A recent example is how DeepMind researchers recently defeated the Alpha Go world champion by training a deep reinforcement learning model to defeat itself and ultimately others through self-play.<sup>[14]</sup>

Today, we see the beginning of ML as a signal modulation (e.g., APSK, PSK, QAM, etc.) classifier. Past approaches relied heavily on hand-engineered feature extractors for specific signal properties along with rigid decision boundaries. These knowledge-crafted detectors created oversimplifying assumptions, making it difficult to adapt to new signals or emitters. Recently, some have trained convolutional deep neural networks (DNNs) with raw in-phase-quadrature (I/Q) data to classify modulation schemes with results well over 80% for high signal-to-noise ratio (SNR)—above 10dB, delivering some promising results.<sup>[15]</sup> Still, these approaches for modulation classification are not without challenges. The current state-of-the-art is only useful at high SNR levels and with higher-order modulations being more difficult to classify at lower SNR. Moreover, the nature of DNN makes explainability and errors difficult to interpret, which affects trust. For instance, there is no set of features a DNN can offer an operator to explain why the classifier reached its decision.

Participants identified three key challenges to employing AI/ML in EW/Cyber operational systems. The first is identifying and developing an infrastructure to support the research and development of these systems. This infrastructure includes the collection and storage of data for ML algorithms; the DevOps environment to support rapid prototyping and testing with this data and other developed models; and the experimentation ecosystem (simulated, emulated, and live) to support the development of operational concepts and to provide feedback to engineers. To that end, the DoD's Joint AI Center (JAIC) is working towards such a foundational infrastructure, albeit perhaps without a focused eye towards some of the implications discussed here for EW and cyberspace operations development.

The second challenge, as with any AI/ML program, is that the data acquisition, ingestion, and curation (a.k.a. the data pipeline) becomes an increasingly important component in building reliable systems. This makes raising community awareness for collecting signal data during operations, exercises, and other activities having signals of interest paramount.



Preferably, data is being labeled as it is collected. Often, it is not labeled, so the generation of synthetic data, where labeling can be easily controlled, becomes a default second strategy. Research must determine how to generate such cognitively plausible data streams with realistic, underlying physical signal characteristics. It must also simultaneously develop techniques to transfer learned AI/ML models, trained by synthetic data or real over-the-air (OTA) signals. Research is also needed to evaluate techniques to speed up learning, such as re-training the last few layers of a deep neural network or compensating for lack of data with generative adversarial networks.

Data and algorithm issues with sensors, storage, and compute locations must also be addressed given the disparity between the low bandwidth, high latency tactical edge and the cloud environment where most development and ML training occurs. For context, learning in AI may occur offline or online. Offline learning involves training the system, typically on millions of samples, outside of its operating environment before it is deployed to the production system (e.g., training a surveillance system with many images). Alternatively, online learning is when the AI system uses continuous data from its operating environment to refine its decision-making parameters. Participants recognized that online learning is important as military operations often occur in austere environments where connectivity to the “cloud” is intermittent at best. The ability for the system to learn online from both environmental cues and operator provided hints, requires other types of AI learning, such as reinforcement and episodic (i.e., analogy-based learning). This type of AI learning’s applicability to signal detection, characterization, and response is not as well studied as offline deep learning approaches.

The above two challenges involve some research but are primarily engineering challenges. The last challenge identified was more fundamental, as it involves the issue of trust between the human operator and the AI system. This challenge is brought up in many other military contexts when talking about the relationship between the human operator and their military tools, such as one’s rifle or tank, so we will not belabor the point here but rather point out some of the unique challenges with AI/ML systems. As mentioned above, the lack of transparency, or explainability, of non-symbolic ML approaches makes it difficult for human operators to understand how the underlying system inferred its classification. Without this understanding, it makes it more difficult for operators, especially experienced operators, to trust the system without a lot of training. Augmenting these non-symbolic approaches with references to symbolic, interpretable representations which make grounded explanations possible, is one approach to mitigate this shortcoming.

Adversarial ML<sup>[6]</sup> is another issue that decreases trust in the AI/ML system if not properly addressed. In effect, adversarial ML is the ability to “spooft” an ML algorithm to classify a sample the way an adversary desires versus the way the model was trained. Through slight, unrecognizable perturbations in the input signal, adversarial ML takes advantage of the model’s classification boundaries, or manifolds, and the model misclassifies the sample.



**Dr. Jacob H. Cox Jr.**, received his BSEE from Clemson University, SC in 2002, his MSECE from Duke University, NC in 2010, and his Ph.D. in ECE from Georgia Institute of Technology in 2017. As an Army officer with 21 years of active service (1996-2018), Jacob has served as a Cyber officer, a telecommunications engineer, and a signal officer. His assignments include company command at Fort Gordon, Georgia (2006-2008); Assistant Professor at the United States Military Academy (2010-2013), and Chief of Enterprise Operations at the South West Asia Cyber Center in Kuwait (2013-2014). Following his Army career, Jacob worked as a research scientist adapting artificial intelligence solutions to cyberspace operations, electronic warfare operations, and decision support. Jacob currently works as the lead data scientist at TCM Cyber, Fort Gordon, GA.



**Colonel Dan Bennett, Ph.D.**, joined the Army Cyber Institute in 2015. He is the Director of Research since serving a one-year operational experience (2016-2017) as the Technical Director Advisor to the Commander of the Cyber National Mission Force at Ft. Meade, MD where he led cyberspace operations infrastructure initiatives in particular. Col. Bennett came to the ACI from the Department of Electrical Engineering and Computer Science (EECS) at the U.S. Military Academy where he still teaches as an Associate Professor. Col. Bennett's previous operational experiences include the lead network engineer for the 101st Airborne Division (Air Assault) which included 15 months as the Director of the Joint Network Operations and Security Center for Combined Joint Task Force – 101 in Afghanistan. Col. Bennett has a Ph.D. in Electrical Engineering specializing in Communications and Digital Signal Processing.



**Colonel (Ret.) Scott Lathrop, Ph.D., CISSP**, is a visionary technology leader in AI, cybersecurity, and autonomous, unmanned systems. Dr. Lathrop retired from the United States Army, culminating his military career as the Director of Advanced Capability and Technology at the United States Cyber Command (USCYBERCOM) where he led the command's research and development efforts while serving as the chief scientist and technology officer for the Commander, United States Cyber Command/Director, National Security Agency. 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 (USMA) helping design and lead USMA's initial cybersecurity and robotics programs. He is a distinguished graduate from West Point and holds a Ph.D. in Computer Science and Engineering from the University of Michigan and received the Army's Draper Leadership Award as an Armored/Cavalry commander, led the development of some of the Army's first cloud-based command and control analytic applications, and has been recognized for teaching and research excellence.



This effect, coupled with the lack of explainability in how these inferences are made can quickly erode trust if the operator suspects malplay. To help build trust, participants expressed the need to bound the behavior of the AI/ML system through interaction and the ability to express what the system's high-level goal(s) and tasks are for the current operational mission—in much the same manner that one would direct a small unit or individual soldier.

Finally, as to the application of AI to enhance EW and cyberspace capabilities, participants asked that leaders and researchers consider which systems and platforms in current use could benefit from autonomy. Participants noted that humans might place too high an expectation on autonomous systems to perform flawlessly and expect too much too soon. They noted that humans frequently fail to perform perfectly, yet autonomous systems seem to be held to a higher standard. These observations drove some interesting questions. First, what level of error threshold are we willing to accept from systems working autonomously? Second, assuming we cannot account for all the system's data in real-time when it makes an error, who gets blamed for the error when it occurs? These are challenges and ethical considerations for future discovery.

## **VII. LEVERAGING EW AND CYBER FOR IO**

US adversaries have already successfully leveraged the cyberspace domain to conduct information operation (IO) campaigns. Due to the restrictions on U.S. military operations from Title 10 (the role of the Armed Forces), Title 32 (National Guard) and Title 50 (National Defense) mandates, the flexibility and options used by our adversaries to gain advantage are not readily at the disposal of U.S. Forces. Given the nature of a cyberspace war that would place U.S. Forces in near constant competition with our adversaries, we must ask what that line of delineation between competition and conflict regarding the execution of Title 10, 50, and 32 operations is? Workshop participants observed that the line between competition and conflict is not easily defined. Given that traditional military operations are addressed and executed through a phased approach, the planning and execution phases of EW/Cyber operations are difficult to pinpoint.

The difficulty in identifying the phases of a war in cyberspace is further compounded when we attempt to apply traditional operational doctrine to the situation, specifically, the execution of IO in accordance with Joint Publication (JP 3-13). It characterizes IO as the integrated employment, during military operations, of Information Related Capabilities (IRC's) in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. The phrase, "during military operations," could be difficult to identify. JP 3-13 goes on to say that many military capabilities contribute to IO and should be taken into consideration during the planning process, including strategic communications, public affairs, civil-military operations, information assurance, space operations, military deception, joint electromagnetic spectrum operations, and cyberspace operations. In this description, cyberspace operations and information assurance are listed as distinct entities from electromagnetic spectrum operations.



**Mr. Chris Walls** is a retired Cyber Warfare Officer and is currently a Lead Cyber Security Engineer with the MITRE Corporation. He was commissioned as an Infantry Officer and served in both mechanized and airborne units with numerous combat deployments. In 2010, Chris began his cyber career at US Cyber Command and subsequently served operational and institutional assignments at Army Cyber Command, Army Cyber Center of Excellence, and in HQDA G/3/5/7 Cyber Directorate (DAMO-CY). Among his many distinguished accomplishments, he most recently led the development of Army Field Manual 3-12 Cyberspace and Electronic Warfare Operations, assisted in the design of the Army's new Cyberspace and Electronic Warfare units, and is an acknowledged expert on full spectrum cyberspace operations within the Department of Defense. The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.



**CW4 (RET) Jason LaClair**, joined the Army in September of 1995 and attended Basic training at Fort Jackson, SC. He then reported to Advanced Individual Training in Pensacola, FL. Jason has been a career military intelligence (MI) Soldier with assignments including the National Security Agency, the Space and Missile Defense Command, the 4th Infantry Division, the National Reconnaissance Office and Army Cyber Command. He has been deployed to Iraq and Afghanistan and served temporary duty in Korea, India and New Zealand. Jason attended the Intermediate Signals Analysis Course, warrant officer Basic Course, warrant officer Advanced Course, Air Assault and Airborne School. Jason's awards include the Legion of Merit, the Bronze Star and the Commander's Award for Civilian Service. Jason has a Bachelor of Science from the University of Alabama and is pursuing a Master of Public Administration from Penn State University. Jason currently works as a defense contractor and resides in Augusta, GA.



**Lieutenant Colonel Clint Tracy** was commissioned from Texas A&M University as an Armor Officer and served in leadership positions in Armor Battalions from 1998 to 2006. From 2006 to 2010 he was assigned to Operations Group, National Training Center, Fort Irwin, California and the Canadian Maneuver Training Center where he served in observer controller positions providing feedback to units preparing for Operations Iraqi Freedom and Enduring Freedom. In 2011 he attended CGSC and simultaneously earned a M.S. in IT Management. From 2012 to 2016 he served as the G35 1st Infantry Division, a Cavalry Squadron XO, Brigade S3, Brigade Deputy Commander, Provisional Brigade Commander, and the Theater Army Branch Chief for TCM EAB. In 2017 he transitioned to Electronic Warfare and is currently the CEMA Chief for the 1st Cavalry Division where he integrates Cyber and Electronic Warfare into tactical operations. LTC Tracy has combat experience in Iraq and Afghanistan.

The mission of ARCYBER is to “conduct full-spectrum cyberspace operations, electronic warfare and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries.” One could argue the mission of ARCYBER is, in part, to conduct IO. Already, ARCYBER is in the process of categorizing many of the separate operations above (EW, IO, and cyberspace operations) under the umbrella of “information warfare.” The term “Information Warfare” is not yet defined in our doctrine; however, the initiative stems from NDAA Sections: 1637 - Integration of Strategic Information Operations and Cyber-Enabled Information Operations; and 1641 - Plan to Increase Cyber and Information Operations, Deterrence, and Defense to Develop a “Strategic Framework for the conduct of DoD IO.” However, according to BG Angle, the role of the ARCYBER Commander may be short-lived, becoming a subset of IO, while the name of ARCYBER could soon become something close to Information Warfare Operations Command.

Recognizing this, a closer look at how and when IO planning occurs is in order. JP 3-13 is clear, “IO planning begins at the earliest stages of [the] Joint Operations Planning Process (JOPP) and must be an integral part of, not an addition to, the overall planning efforts. IRCs can be used in all phases of a campaign or operation, but their effective employment during the shape and deter phases can have a significant impact on remaining phases.” When do these “shape and deter” phases begin and end? The conduct of IO must have an appreciation for the inter-related capabilities of cyberspace operations, (both defensive and offensive), EW, and signals intelligence—most importantly for assessing the effectiveness of IO. Due to the length of time needed to identify, develop, and deploy cyberspace operations tools, waiting until phase 0 to begin the process (especially the process of collection management from an intelligence perspective) will likely not deliver the desired effects when needed. Perhaps no kinetic operation is warranted if a shape and deter IO campaign is effective in quelling any conflict before it begins.

The Army, specifically the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO-IEWS), views Information Warfare as the complementary components of intelligence, cyberspace operations, EW, and signal. Each of these elements is a potential tool for conducting Information Warfare. With that, the acquisitions process is being adjusted to meet the needs of warfighters with more agile acquisition processes and best-of-breed application of commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) capabilities. One expects the doctrine to evolve with the capabilities. Cyberspace operations and capabilities will also impact the Commanders’ decisions in the arena of “intelligence gain/loss” like never before. New questions will seek to determine whether the delivery of content in an IO campaign will rival the Commander’s ability to disable an adversaries’ communications network? These are challenges that U.S. commanders have not faced on linear battlefields in the past, but emerging technology is bringing enhanced cyberspace and EW operations to the forefront.



**CW4 Judy Esquibel** is an active duty Cyber Operations Technician. She is currently assigned as an Information Sciences Ph.D. student, at the Naval Postgraduate School, Monterey, CA. Formerly, she served at the Army Cyber Institute (ACI) and as an Instructor within the Electric Engineering and Computer Science Department, U.S. Military Academy, West Point, NY. Her research efforts at the ACI focused on improving critical infrastructure protection, public-private partnerships and cyber exercises. Some of her results and conclusions were codified in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to enhance the nation's critical infrastructure security. Her operational experience includes 20 years of Signals Intelligence and Cyber operational assignments, which include being assigned on a Combat Mission Team, within the Cyber Mission Forces, U.S. Cyber Command.

Cyber is inherently a joint operation. Just as the Navy has re-badged numerous elements within their formations to present a better-defined mission focus, and consolidate talent and resources, so too shall the Army. Challenges facing the Army will be which flags are to be furled and which are to be flown. As the Army decided between intelligence and signal to give birth to a cyber element, similar decisions now must be made about acquisitions, requirements, training, and doctrine supporting elements. Training must be the most pressing item. Is this a maneuver effort, an intelligence function, or a cyberspace operation? A kinetic or non-kinetic fight? Is the Information Officer on staff equipped to take on such a task? Cyber Intelligence is not a recognized category, but the operational information gleaned from cyberspace operations certainly carries intelligence value. How is the relationship between the staff intelligence officer, operations officer, and signal/communications officer meeting the commander's requirements to protect his or her network while potentially exploiting or denying the adversary use of their own? Cyber Electromagnetic Activities cells (see FM 3-38) are operational elements at the Division level, but the IO campaigns from which they feed and obtain information will likely be conducted at the theater level.

The categorization of IO as a kinetic or non-kinetic capability is not a simple task. If, when learning that an adversary has disabled a Bradley via a cyberspace operation (a phase 0 activity) in an information warfare campaign and the crew then abandons that Bradley, the vehicle is effectively destroyed, similar to a kinetic effect. Adversely, if counter-cyberspace operations (defense) are effective in keeping the adversary from disabling the Bradley vehicle, it can deal a blow to the adversary's battle plan, both kinetically and from an information warfare perspective. Then, how useful can efforts before phase 0 of an operation to obtain the information needed to access networks, impact social media users, degrade GPS, or disrupt communications? The simple demonstration or application of these capabilities may negate the need for

further escalation. Perhaps these efforts could be the decisive actions during phase I, II, III or beyond in the Operation Plan (OPLAN), but they would not be available if the planning phase was not enacted until phase 0. Part of the challenge will be proving that the desired effects can be met via cyberspace operations where kinetic effects have traditionally persevered. Combatant Commanders trust visuals of smoking craters more than percentages (or probabilities) of success based on mathematical equations. This will require the inclusion of new, modular, and data-driven battle damage assessment (BDA) tools for IO.

In closing, leveraging cyberspace and EW operations to facilitate IO opens a wide spectrum of possibilities to warfighters, potentially winning wars before they are fought. Already, EW is listed as one of the five core capabilities of IO.<sup>[17]</sup> At a minimum, conducting IO at the earliest possible opportunity will give Commanders an advantage during subsequent phases of the battle. However, the correct characterization and application of IO are required. The manning, training and equipping of those expected to execute IO also deserves appreciation and attention by commanders and given a priority of effort.

## VIII. CONCLUSION

As near-peer adversaries continue to develop and employ increasingly advanced technologies in multi-domain battle, the US is challenged to hone its EW and cyberspace operations into carefully integrated capabilities. Naturally, the merger of EW and Cyber comes with challenges, friction points, and gaps that must be overcome for U.S. Forces to thrive in multi-domain battle. The EWC2 workshop identified multiple challenges and opportunities where these issues can be addressed. As such, this work merely offers questions and leaves the real work to other researchers, policymakers, and leaders to answer. Additionally, while the EWC2 workshop's focus began with the convergence of EW and Cyber, it is apparent that even these may only be part of the larger whole. In the future, other components, such as IO, Psychological Operations, Intel, Space, and Signal, may soon join the merger.

Participants also discovered that the Army is already conducting a study to ascertain how all of these groups might fit under the umbrella of Information Warfare Operations. Perhaps a circus tent would be apropos considering how these disparate disciplines must learn to complement one another. Regardless of terminology, the concepts behind Information Warfare Operations must be further refined. To accomplish this feat and dominate future conflicts, the U.S. and its allies must work together to address friction, close gaps, and embrace evolving technologies within EW and cyberspace operations, incorporating other disciplines where it makes sense. With near-peer adversaries investing in EW and cyberspace operations, rapidly building and employing their capabilities, the U.S. must aggressively tackle these challenges or face a future conflict where information superiority is not achieved. 🛡️

## **ACKNOWLEDGMENTS**

The authors would like to extend our thanks to the organizations and individuals who contributed to the workshop's success. This workshop would not have been possible without the support of the Army Cyber Institute (ACI) at West Point, NY and the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center at Aberdeen Proving Ground (APG), MD. We especially thank our volunteers MAJ Joseph Kosturko; Mr. Giorgio Bertoli, CPT Ian Bolster, CW2 Brandon Chapelo, CW3 Benjamin Holladay, Ms. Caitlyn Byrne, and Dr. Michael Lilienthal for their leadership and assistance with the working groups.

## **DISCLAIMERS**

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

*Approved for Public Release; Distribution Unlimited. Public Release Case Number 19-2915*

## NOTES

1. Field Manual, "FM 3-12 Cyberspace and Electronic Warfare Operations," April 2017.
2. CERDEC has since been rechristened as the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center.
3. Cyber electromagnetic activities (CEMA) are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0).
4. Some refer to these types of non-physical engagements as "non-kinetic", for example see [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2474091](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474091).
5. S. Cohen, "Integrating Cyber and Electronic Warfare," *The Cyber Edge*, Signal, March 2018.
6. Joint Chiefs of Staff, "Joint Publication 3-13.1 Electronic Warfare," February 8, 2012.
7. Joint Chiefs of Staff, "Joint Publication 3-12 Cyberspace Operations." June 8, 2018.
8. M. Senft, "Convergence of Cyberspace Operations and Electronic Warfare Effects," *The Cyber Defense Review*, January 4, 2016.
9. P. Frost, C. McClung, C. Walls, "Tactical Consideration for a CDR to Fight and Win in the EMS." *The Cyber Defense Review*, Vol 2 No.1 Spring 2018.
10. "Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)," Combined Arms Center -Capability Development Integration Directorate (CAC-CDID), December 2010.
11. D. Johnson, "Fort Gordon kicks off 2018 Cyber Quest." NextStar Broadcasting, Inc. June 22, 2018.
12. "CYBER BLITZ." Combat Capabilities Development Command C5ISR Center, U.S. Army, [Available] Online [https://www.cerdec.army.mil/inside\\_cerdec/cyberblitz/index.php](https://www.cerdec.army.mil/inside_cerdec/cyberblitz/index.php).
13. S. Trent and S. Lathrop, "A Primer on Artificial Intelligence for Military Leaders," *Small Wars Journal*, August 23, 2018.
14. David Silver, Julian Schrittwieser, Karen Simonyan, Ioannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert, et al., 2017, "Mastering the Game of Go without Human Knowledge," *Nature* 550 (October), 354.
15. Timothy James O'Shea, Tamoghna Roy, and T. Charles Clancy, "Over-the-air deep learning based radio signal classification." *IEEE Journal of Selected Topics in Signal Processing* 12.1 (2018), 168-179.
16. Daniel Lowd and Christopher Meek, 2005, "Adversarial Learning," In *Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, KDD '05*, New York, NY, USA: ACM, 641-647.
17. Joint Chiefs of Staff. "Joint Publication 3-13.1 Electronic Warfare," February 8, 2012.





# Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate

---

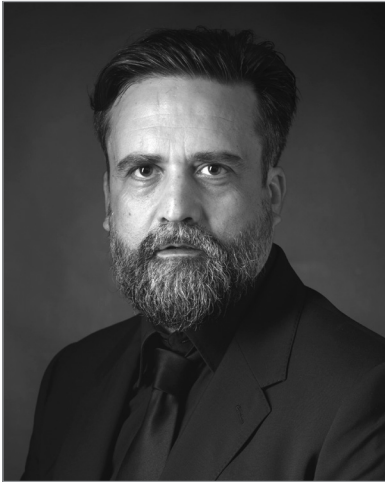
Rudy Guyonneau  
Arnaud Le Dez

## THE SAME OLD HUMANS IN A BRAND-NEW, DIGITALIZED WORLD

**T**echnology changes our world at such a rapid pace that our natural, human intelligence has a hard time coping with its brutally disruptive evolution. The transformations of digital technologies have made deep and lasting impacts on our societies. Information, which is at the heart of the last century's technological developments, has become such an essential resource that it is now a component of power. Information exchanges have sped up and intensified, which has resulted in a loss of culture as societies have become more uniform. Cyberspace, which appeared in the blink of a geologic eye, has become a favored way to communicate because of its ease, accessibility, and global range.

Despite advances in technology, humans remain the same at their core. Cyberspace has become a confrontational place where ideas and wills oppose themselves. Alternate "truths" have found a way to express themselves unrestingly there, thus producing discord. Unlike the dream of the generation that created it, cyberspace is not a world of peace and of universal harmony. Because this new, digital world can also carry the expression of an adversarial will, it thereby becomes mandatory to manifest oneself there, in order to fight it. From now on, one must be in capacity to take action in cyberspace, to act upon information if not on the means to process it. And sometimes, to impose one's will, one must move towards war. While an actual war has yet to occur, the military is already engaged in digital warfare. At first, cyberfighters acted independently, but are now integrated into the combat forms of the land, sea, air, and space domains. It is the cyberfighter's duty to support and augment physical battles in those domains. Cyberfighters, in contrast to their military brethren, can sustain a form of permanent conflict against non-state political entities without ever having to declare war. Digital warfare is indeed a long-haul fight, with the objective of weakening adversaries in cyberspace to win an advantage in military, economic, political or societal spaces.

© 2019 Dr. Rudy Guyonneau, Arnaud Le Dez



**Rudy Guyonneau** is a Senior Consultant in Artificial Intelligence for Cybersecurity at Sopra Steria SA. His doctorate thesis with Spikenet Technology at the Brain and Cognition Lab in Toulouse led him to study visual information processing in the primate's brain, to apply its keys in the fields of Machine Vision and Neuromorphic Engineering. After postdoctoral research at Georgetown University on Brain-Computer Interfaces, he eventually led the R&D effort at Spikenet Technology, applying spiking neural networks and related technologies to the industry, among them, Videoprotection. He joined Sopra Steria in 2016 to accompany the development of AI within Cybersecurity and to assist Airbus Commercial Aircraft in its Innovation strategy. He holds a PhD in Computational Neurosciences from Toulouse III University and acts as the Lead Cyber Data Scientist on behalf of Airbus CA.

As humans are not physically present in cyberspace<sup>1</sup>, digital warfare is inherently technical. This does not mean it is an obscure affair of engineers withdrawn into some virtual tower. Plenty of military-specific concepts maintain their meaning in cyberspace. Military people engaged in cyberspace nurture the understanding of combat at every level, from tactical to strategic. Digital warfare is also a matter of defense and of attack, and ought to be fully integrated with global maneuvering, for the benefit of all fighters. The security team's duty is to outfit the corresponding cyber-ground so that it supports fighters engaged on land, in air, at sea or in space. The cyber-defense team hunts the attacker with the intent of disarming or weakening it. Such a defense can sometimes lead to cyberfighters acting beyond the digital frontline, in gathering intelligence or enforcing power. Right at the heart of digital warfare, in the very fabric of the space itself, cyber-fighters can find information and data. The growing automation and interconnectivity of military equipment multiplies the importance of information control—it is a key to power.

At the same time that the conditions for digital warfare emerged, automated information processing capacities experienced a qualitative leap. Artificial intelligence (AI) can thus be found at the heart of cyberwarfare because of its perceived potential and inherently numerical nature. Its impact over our hyperconnected world makes us interrogate ourselves to determine what constitutes humanity. From initially being the focus of academics, AI has quickly become the center of industrial interest and public expectation. The question of AI now tends to manifest under the guise of a mythicized omniscience and therefore, of a mythicized omnipotence. This can lead to paralysis of people fearful of having to fight against some super-enemy endowed with such an intelligence that it would leave us bereft of solutions. If this anxiety can be

<sup>1</sup> In France, the « *espace numérique* » is thought of as composed of three layers: physical, logical and informational. Humans and, through information, their perceptions become a target via the third layer. Humans are thus present in this part of cyberspace but remain less representative a function in a world that is inherently electronical. Combat remains in *fine* the matter of a dialectic in-between human wills.



**Arnaud Le Dez** is a French officer assigned to the Center for Doctrine and Command Teaching (CDEC) of the Army as a cyber defense expert. He started his military career in electronic warfare and information system administration and security, then switched from operation duties to headquarters positions, and was involved in several external missions in Lebanon and Afghanistan. In 2010, he joined what would later be known as COMCYBER and held various positions in cyber defense operations. Arnaud Le Dez holds a specialized Master's Degree in "Operations and Crisis Management in Cyberdefense" from Ecoles de Saint-Cyr Coetquidan. He is also an associate researcher at the "Mutation of Conflicts" division of Ecoles de Saint-Cyr Coetquidan Research Center. He authored "Tactique Cyber, le Combat Numerique," published in January 2019 at *Economica*.

understood, then the high stakes around the AI question become clear and must be addressed with reason.

Digital warfare and artificial intelligence share the same space—electronic equipment—and the same representativeness—digital. But what relationship do they have? How could this translate onto the field? What could it mean in the long-term? Here, we try and reframe the debate on rational and concrete grounds, which eventually led us to the vision of a cyber teammate. We do this because, in order for digital warfare to utilize AI and grow as a capability, and hopefully, as a force, we must have a grounded stance.

### *Digital Warfare: A Fight Like Others*

Like other forms of combat, digital warfare is defined by its environment. Cyberspace grows by the interconnection of information systems of all kinds—business systems, as well as industrial and military ones—that form global networks. It is a medium for storing and making the quasi-instantaneous exchange of information that humans rely on daily. The information stored ranges from the most intimate testimonial to political action to economic, diplomatic, strategic, and tactical exchanges. It can be a tremendous echo chamber for communities of people and offer a way for the most vulnerable populations among us communicate and advocate. Cyberspace is not the exclusive tool of the mighty; it can enable the emergence of evil or benevolent organizations and ideas by connecting otherwise isolated individuals.

As an integral part of joint and tactical maneuvers, the operations and missions that utilize digital warfare are planned according to their expected effects within cyberspace or beyond. In and of itself, cyberwarfare is combat, which requires a planned and targeted process to conduct operations. It also requires intelligence at the tactical, operational, and strategic levels to measure its efficacy as well as its own rules of engagement. In cyberspace,

the fog of war is induced by its very nature as a dense, complex, and heterogeneous web of data where stealth and swiftness reign. The limits commonly associated with digital warfare (non-permanence, measure limitations, machine-scale speed, and anonymity)[1] stem from this fog of war. Yet it is possible for one to grab onto and rely on recurrent signals amidst the fog of cyber warfare. In its purest form, it is an insurrection/counter-insurrection type of fight where the weak attacks and the strong defends. Indeed, defense always has more strength, as it has control over its own system, in a physical and a digital sense, which enables it to oust the attacker, including through the radical maneuver of replacing all of the hardware and the software by different equivalents.[2]

### *How The Traditional Principles Translate In Cyberspace*

The principles of digital warfare still need to be codified. Their origins can be found by studying what has actually succeeded on the field, although there are too few examples so far to make any generalizations. Still, techniques and strategies evolve at a frantic pace, the former through the exigence imposed by early experiences in the field and the rate of technological development, the latter as our understanding of the stakes grows. The tactics of digital warfare are still developing, but can rely, at least partially, on the logics established by other warfare domains. Despite its youth, digital warfare can be thought of in relation to trends, and discovering the parallels to guide us. According to the ancient foundations laid out by General Ferdinand Foch in the early twentieth century, the French Land Army relies upon three principles that stem from the legacy of land conflicts: freedom of action, economy of means, and concentration of efforts.[3] The first two have a direct expression in cybertactics, while the third one is harder to distinguish.

- ◆ Freedom of action corresponds to the capacity given to achieve the mission. This is where strength can be found. A physical capacity in its original form, its cyber counterpart points directly to capabilities. Hence, according to the picture drawn above, strength lies predominantly on defense.
- ◆ Economy of means corresponds with reaching the best effects-to-effort ratio within the means available. Since wars are long, longer than battles, and since digital combat remains a human affair, as techniques and operations are led by humans, the economy of means remains one of the principles of victory. Time appears as a center of gravity, around which to apply the economy of means in order to win the fight.
- ◆ Concentration of efforts corresponds with the convergence in time and space of the actions and effects of the involved operational functions. Now, the digital space is constantly changing as it is less material than the natural space where the principle was forged. And time... what is time in cyberspace anyway? One can consider a subpart of the problem, however: combat speed, for example, it is definitely not determined by the speed of the cyber ammunition.[2] As far as we know, speed comes from decision-making, planning,

and implementation, just as in classical forms of combat. One can infer that a, if not the, concentration factor is the person or people overseeing a project. This person is situated at the core of the action, and is essential in controlling the tempo, maintaining the initiative, and keeping focused on precise actions. Taken at large though, concentration of efforts remains less distinguishable, because of the digital nature of the cyberspace.

The digital warfare principles question remains open because of the nature of the field, while being the focus of ongoing reflection. Even though its principles are yet to be firmly established, it nonetheless requires a means of organization, that can be refined as our understanding broadens. What we know for sure, and for now, is that decision-making speed must be prioritized. Decision-making means information-processing. The mind-bendingly rapid development of information technology we are witnessing in this early twenty-first century—best exemplified by AI—can be expected to weigh heavily onto a form of combat that is in its early stages.

### *From Machine-Intelligence to the Intelligence of Machines*

Artificial Intelligence is a technology. It is, by definition, the science of information processing. If the Dartmouth conference baptized AI, its birth can be traced to the seminal “Computing Machinery & Intelligence” paper by Alan Turing in 1950.[4] AI captures some computable aspects of cognition in mathematical form. These aspects of cognition pertain to the acquisition, representation, and production of knowledge. In one instance, it translates in the automation of logical rules, better known as the “symbolic approach.” It is found across the entire spectrum of programming and it manifests itself in the von Neumann information processing architecture that we still call a “computer,” and which now takes the shape of smartphone, a fridge, a vehicle, or a weapon system. Note here that a computer is seen as the materialization of a Turing Machine—a machine capable of simulating any kind of algorithm.[5]

The intelligence found in a symbolic AI is programmed and automated by humans. Machine intelligence relies on the subjective experience the programmer had with said problem. Machine intelligence is constrained by the logical formalism of the language and device by the programmer, which means that its behaviour model is strictly bound by human experience. As a result, the machine is able to replicate human expertise onto a defined world, but lacks any capacity to predict outside of it.

The novelty lies in the implementation of programs that allow machines to learn their own model. Under the term “Machine Learning,” one finds a machine’s capacity to develop its own responses to its environment, rather than relying on specified responses to a given set of symbolic inputs. Humans specify an architecture for the machine to learn an optimal behavior, as measured through an error function. This information processing paradigm appears during the 2012 ImageNet challenge, when Geoff Hinton’s team demonstrated the power of what would become “Deep Learning” (DL) by winning the competition. The success of the “Machine Learning” approach is due to three factors which have become its pillars:

sophisticated algorithms (prominently, neural networks), cheap, parallel, computing power, and a sufficient amount of data describing the activity at hand. This is the ACD triangle. Programmed in this way, the machine has the capacity to unearth relations within the data that would have escaped the expert's attention, because of the following:

- a. The number of channels a machine can analyze at any given moment is much higher (spatial dimension) than what a human could analyze.
- b. The characteristic signal is too weak to be perceived on a single occurrence (temporal dimension).
- c. The expert excludes significant channels because they do not correspond to his or her expertise (cognitive dimension).

If its creation, and sometimes its inspiration, is and remains human-driven, we are dealing with a budding machine intelligence. Yet one has to bear in mind that in no way is the resulting machine "autonomous," "free," or "possessing a will of its own."<sup>2</sup> The reason is simple: AI as a technology maintains a tool-to-crafter relationship with humans. In other words, AI machines are strictly the byproduct of human intelligence, which makes the latter responsible for every aspect of the formers' design, development, and deployment. Thus, it is early to assert machines will eventually surpass and annihilate us. As a technology who originates in a cognitive rather than physical capacity, one can, and actually should, conceive AI in a dialogue with natural, human intelligence. Its products are not "beings," even if the idealization is understandable. They are tools, and in the case of warfare, weapons. The so-called annihilation through AI would be ours, not AI's.

More concretely, the historical perspective presented here reaffirms the sometimes overlooked "software" reality of AI<sup>3</sup>, even though there is a quantitative leap at the functional level. The "new" AI is bound to be deployed in all computers, to gather data. This reframing brings a remarkable insight as to how to utilize it for digital warfare.

### *The Cyberteammate at the Heart of the Digital Warfare-Artificial Intelligence Dialectic*

Convergence between digital warfare and Artificial Intelligence starts in the very space where the former happens. When one considers AI as the science of information processing, then AI is the origin of cyberspace, since it proceeds from computers and their interconnection. It has allowed humans to multiply and automate their exchanges, thus generating such an impressive amount of data that AI was able to enter a second age, that of learning. In return, one can sense that an impact that AI will have on cyberspace will be to extend the machine's operational field to the natural space itself.[6]

Within the context of digital warfare, the amount, complexity, and heterogeneity of data, and the speed of acquiring and processing it, form the cyber fog of war. This data is generated by machines, upon which humans act to manifest their will throughout cyberspace. Where

<sup>2</sup> Not to mention that scientifically speaking, how do you compute autonomy, freedom or will? Desire?

<sup>3</sup> Precisely « computational », but strictly limited to the software level for the sake of argumentation, in waiting for its passing onto the hardware level.



cyberfighters are concerned, capabilities are computers and ammunition, pieces of code: these are inherited from AI's early paradigm. How will the new AI paradigm impact digital warfare then? Machines now have the capacity to make sense of a set of data that is too much for a human to comprehend, even with early-age equipment. AI speaks the language of machines and will translate it for humans to conduct their fight within a machine space.

The cyberteammate is the application of the AI technology for cyberdefense purposes. It is software for now and it provides a unique, and otherwise lacking, sense of the environment to the cyberfighter. With the conditions that learning algorithms are ready, computing power sufficient, and data available, AI will offer myriad applications for cyberdefense. Through AI, the cyberteammate will build its own understanding of cyberspace and will support the cyberfighter by giving them a clear perspective and understanding of the conflict. In this way, it can heighten the intensity of cybercombat, thereby reaching its potential as a planned, commanding fighting capacity. The cyberfighter is appropriately named, as a part of cyberspace and a budding intelligence that will bloom depending on the accompanying conditions, it will support the fighter to accomplish its mission.

Cyberspace is mostly an immaterial space: non-natural, logical, comprehended with one's mind. This is why electronic warfare and perception combat are intimately bound to cyber. It highlights the oftentimes non-physical nature of digital warfare, as it rarely moves into the material world, wrecking destruction on physical objects<sup>4</sup>. On the other hand, AI is an attempt at automating some facets of the human mind. As we can see, these two disciplines, which can be conceived as separate when reduced to their technical aspects, are intrinsically bound one to each other. They co-evolve around a cognitive axis. As sharing a common technical and cognitive cyber nature, it makes the most sense to heavily invest in AI's development for digital warfare.

### *Augmented Intelligence*

Intelligence is key to successful combat and maybe be even more important to cybercombat than other forms of combat. In cyberwarfare, intel is data, collected in cyberspace. Cyberfighters need to know about their adversary's silhouette, weapons, and action modes (IOCs and TTPs), and must be able to characterize the operational theater in terms of environment, culture, economy, etc. At the tactical level, gaining intel is an aspect of combat itself. Intel provides the cyberfighter with an understanding of what is happening on the cyberbattlefield and in relation with the physical world. It is achieved at the tempo of combat, so that the officer in charge conducts it within the joint maneuver. Good intel is the sign of the strong convergence between AI and digital warfare, and its most obvious application can be found in the evolution of Natural Language Processing.

Swift, flawless, automated translation is expected by the intel world. Based on the advances in analyzing unstructured data, and the growing capacity to output in a given language, AI will help overcome the cultural barrier to conducting research and, more importantly, interaction.

<sup>4</sup> The physical treatment of cyberspace infrastructure might be a necessity of combat, but is not at the heart of its vocation.

A cyberteammate for intel would rapidly collect data across an otherwise unaddressable range of open sources, translate and synthesize it in a short paragraph, provide a status and isolate the tactical and technical information relevant for combat. It would also improve its capability of cultural influence through social media by automating part of the translation process and simulating more credible legends to magnify the impact of inflammatory posts. It can be deployed passively, as when it assess massive amounts of open written text as it is able to detect changes in tone or style, and link together different texts written by the same, anonymous author.

Situated at the heart of combat itself, augmented intel can dissipate the fog of war, resulting in a swifter and more just attribution. AI's capacity to address vast amount of data has a natural application in the data analysis performed to a battlefield's situation. When data relative to the combat zone is analyzed in its entirety, it can produce a complete and precise picture of the situation. The cyberteammate also contributes by establishing a situational map of operations on the battlefield, accounting for the battle's history and progress, perhaps to the point of actually predicting its evolution, at least in the short-term. Attribution is an exercise in nuance rather a binary one[7]; attribution increasingly relies on a given data, analysis of its timecourse, studying its interactions with the surrounding data, and addressing it within the global context while utilizing intel from sources other than cyber.

### ***Simulation and Customization***

If the corresponding data exists and can be acquired, a cyberteammate has the capacity to simulate any type of environment, whether friendly, neutral, or adversarial. These simulations improve the training of cyberfighters by designing a more realistic operational theater as well as a more complex opposition; one can relate here to Reinforcement Learning and its achievement in the GoGame, as well as to Generative Adversarial Networks.[8] These platforms recreate scenarios that have been encountered in the field to explore the consequences of choices other than the ones that were made.

Prior to combat, the simulation allows fighters to rehearse with action modes and weapon types tested in realistic wargames. The damage output and the expected effects can be measured, studied, and validated and their results can then be integrated in the global planning. Non-compliant cases can be tested and others discovered. The cyberteammate provides simulation support during operations as well, by predicting outcomes based on data gathered and analyzed. AI will never be omniscient, and it will not replace humans, especially in spheres like combat, where determination, strength, and passion are necessary to succeed. Emotions and such characteristics are simply not computable, at least right now. Cyberfighters can choose to heed the advice of a digital teammate, or dismiss it. The challenge will be for us to understand its limitations, biases, and difficulty assessing an enemy we might not recognize; we will have to learn to "talk" to it.



### *The Tactical Cyberteammates*

Digital warfare can be broken up into three tactical modes. The security mode sets up the combat zone and makes it defensible. It checks for good cyberhealth that enables operations and increases the accuracy of attack detection systems. AI can give this mode a camouflage capacity. Once it learns the global behavior of the system it secures, the cyberteammate computes and produces the counter-data necessary for smoothing out the data produced by the securization activities. If the enemy is already within the system, the objective here is to keep the installation invisible, so that the environment seems to be performing as expected, while it enables a strong defense and prepares for a counter-attack. The element of surprise is also a winning factor in digital warfare.

A defensive mode starts with detecting an attack. AI contributes both legacy-wise and novelty-wise. The “honeypot” evolves to enact human-driven and somewhat credible target systems, luring the attacker into taking possession of it. The gain is two-fold: an extension of the domain to defend while shortening the actual attack analysis. AI also brings the possibility of a defense cyberteammate that mimics the defensive stance of a cyberfighter. Such a deployment would act as a first defense layer allowing the human teammates to focus on assessing the global situation and defending more critical systems, both of which are in line with the freedom of action and the economy of efforts principles.

In the offensive mode, the cyberteammate deploys another form of camouflage. Having learned the language and the operating mode of the target, it applies them to the commands to make them invisible. AI can suggest which commands to give, but the ultimate decision is up to the human fighters. Additionally, the maneuver itself can be fortified by an attack by cyberteammates, which would simulate aggressive behavior and divert the target’s attention. If cyberfighters choose to run this type of diversionary tactic, they must give special attention to this type of system as it could potentially hinder the maneuver with undesired affects. The offensive cyberteammate embodies the question raised by AI’s advanced weaponry and by extension, of their autonomy.

### *Limits and Perspectives for a Cyber-Oriented AI Development*

AI is a technology. It is peculiar in that it reflects us back to ourselves and leads us to believe it might be, if not alive, then animated. It does not have to be this way. Anthropomorphizing AI inflates it into some sort of omniscience, a sure sign the “Peak of Inflated Expectations” of the Technology Hype Cycle has been reached. But these outsized expectations always meet a “Trough of Disillusionment” when the early experience fails to meet the expectations of exaggerated marketing campaigns. Now that most technologically advanced nations are strategically planning at the highest levels—without myths but with a strong set of values and knowledge—we can expect that we are starting our way up the “Slope of Enlightenment.” Presently, the focus is to design AI on a sound basis, for a concrete and rational adoption on the ground.

AI's strength relies on three pillars: algorithms, computing power and data, all of which are enabled by humans. AI's strengths are its weaknesses, which we will address, in part, and suggest some potential remediations.

- ◆ **Algorithms:** “Deep Learning” is the most representative type of Algorithm. These are highly-nonlinear so are hardly explainable, if at all. Devoted programs have been launched to tackle this problem (e.g. DARPA's Explainable AI). The rule is for the operational deployment of AI to be effective, controlled and simple. While perfectly reasonable and legitimate, it is a bit of a paradox, as AI is here to develop its own understanding of the vast amount of a data we can no longer handle. We may not need to be able to explain its reasoning in order to be confident in its outputs; we might rather learn to understand and get used to it through training and education. Mostly, we need to keep it in its proper place, that is, not in control.
- ◆ The demand for **Computing** power is voracious and requires cloud-like capacities. This solution induces additional delays at the tactical level of combat, especially when moving rapidly. Aiming at local, modest applications could actually help AI-enhanced cybertroops remain within the required tempo. Besides, the simplicity of these applications would advance AI adoption by field personnel, whose operational skills tend to be stronger than their tech-savviness.
- ◆ The capacity of AI to account for excess **Data** opens the door to data-manipulation by its very environment[9]. Maintaining the integrity of the data should always have the highest priority, as the consequences of it being tampered with will be equal to the power it could give. A robust algorithm will partially protect the integrity of the data, but quality sensors should also be involved.

AI is also a science. It advances our understanding of a given topic—the processing of information—and bounds our knowledge through the use of reason. This means our concerns, and sometimes our fears ought to be addressed rationally. AI's development should be embraced because of its potential to be a solution to a cyberspace that appeared too swiftly for the human brain to adapt to and to make its own. Because it is cognitive, and the brain is where cognition naturally happens, AI may be considered an extension of the brain, as foreshadowed by the Neuralink initiative, or DARPA's Intelligent Neural Interfaces program. But let us not forget the pioneering work of Miguel Nicolelis and his team in 2003.[10] It is remarkable that the media makes such a huge use of the brain imagery when discussing AI, and that AI development seem to devote little attention to neurosciences, a discipline which contributed to AI's inception,[4,11] and is at the core of AI's recent progress (DL replicates aspects of the human visual system),[12] and continues to deliver insights.[13] The military, especially, would benefit from using biology, and the neuromorphic engineering sprouting from it, as this has economy of means, both energetic and computational (e.g. IBM's SYNAPSE program).

### *What's Next for Digital Warfare*

Digital warfare is a form of combat, just like more traditional forms of combat. It is highly technical and successful digital warfare requires a tactical sense and strategy, placing it squarely in the military realm. It draws its tactical principles from land, air, sea, and space legacies. AI plays a role at every level of digital warfare, from hunting the enemy through sensors and gathering intel, through assisting in decision-making and simulations, to supporting the maneuver and use of cyberweapons, and more. In its core capacity of addressing the fog of war, AI offers a possible solution—even if only partially—to the non-permanence, the measure limitations, the machine speed and the anonymity that characterizes cyberspace. Efforts to develop AI within the context of digital warfare are strategically important. These efforts will maintain our combat capability in this newly emerged battlespace, while becoming a component of power in all the others.

As mentioned above, the ACD pillars offer many research pillars for increasing cognition degree—synonymous to an increasing degree of automation—to the point of possibly culminating into a real form of autonomy. Military-specific investment in these research pillars is necessary, for the sake of sovereignty and for practical purposes as well, as cyberfighters will make use of AI in rugged conditions. Data-centric development indicates that a dedicated line of operations will be allocated to maneuvering the sensors in charge of collecting data. On a global level, this applies to cyber-oriented intel. This development is a necessary step to get digital warfare to reach its goal of a full and seamless integration within other military operational domains.

Let us not forget the central actor: the humans who forge AI, in order to fight with it. The quality of cyberteammates will depend on the quality of the scientists who conceive them, the quality of the engineers who build them, and most of all, the quality of the military personnel who command their design, their deployment, and their use. The military must take ownership over the development of cyberteammates, in order to guarantee that the technology follows the values the military is sworn to defend, while remaining accountable for its use and effects, in line with the law of war. Without safeguards such as rules of engagement, the introduction of AIs on the battlefield could, and would, instigate a rise of undesired extremes on either side, or, at the very least, a rise in aberrant behaviors. But again, as humans are in charge of the design, the development, and the deployment of AIs, they also must be accountable for their machines' behavior. The machines' display of intelligence means that we can never forget that they are weapons, whose creation and continued existence is our responsibility. If we cannot guarantee the behavior of a weapon, we should not be allowed to use it. The dominion of will, and its rights and responsibilities, is and must remain supremely human.

### *To Choose is to Become*

The excitement in building a new capability lies in the freedom of imagination and, its success lies in developing a profound knowledge base in a variety of fundamental sciences such as military, computer, mathematics, cognitive, social, etc. It is a time for dialogue, of sharing ideas and confronting intuitions, collaborating with experts in other domains to work through intellectual deadends. Although the journey is exhilarating, there are pitfalls. The trick is to let go of our anguish, our fears, our resentment, and of our *own* biases; and to stay anchored in reason.

It is far too soon to predict what the future holds, as this is only the beginning of the intelligence of machines. Left to others, AI will materialize as the scary figures they propose. The choices we now make as brains and machines hit their strides around the world will shape the AIs we will adopt on tomorrow's battlefield. One culture's choice of an AI will not be the same as another's, whose approach to cyberspace will differ similarly. Let us remember, in a bid against any distractive anthropocentrism, that cognition is the hallmark of living things, not uniquely of humans. Tomorrow's AI will have the whole range of biological forms to take inspiration from. Why have expensive terminators when you can have easily replaceable swarm of automated killer bees? More seriously though, future digital warfare will have a wide array of approaches and technical choices available, will share a common data-environment, and still be deeply rooted in previously defined objectives and frameworks. Let us reassure Clausewitz and his heirs: because AI is conceived by humans, warfare will remain a combat of human will.

AI and cyberdefense are complex and emerging disciplines. They require quick responses, to account for the pace at which they are being developed, yet these responses must be thoughtful and well-reasoned. The early reflections presented here raise far-reaching questions, and we hope that they will help with the concrete and conceptual development of AI and cyberdefense. Mainly, we show that digital warfare and artificial intelligence converge in cyberspace—the former by expressing our will, the latter by supporting it. Their importance lies in the advancement of knowledge that will happen with their development and the power they have on the battlefield. We should support ambitious research and supervised development to support their growth into maturity and to frame AI in accordance with the military's goals. The force of digital warfare resides in the capacity to analyze and act on collected data, rather than in merely possessing it. AI, the science of information processing, has a key role here.

As a final note, we would like to take a step back and consider the state of the public debate. AI tends to manifest itself under the guise of a mythicized omniscience, and thus omnipotence. AI is not a god; it is a forge and data is its fire, hardware its anvil, and algorithmics its hammer. The weapons in the future will be a myriad, and the cyberteammate who can fight alongside the cyberfighter will be the most remarkable of them all. AI is the key to cyberspace's intelligibility. Without it, digital warfare will endure; with it, it will thrive. 🍷

## NOTES

1. Kallberg and T.S. Cook, (2017), The Unfitness of Traditional Military Thinking in Cyber. *IEEE Access* 5, 8126-8130. DOI: 10.1109/ACCESS.2017.2693260
2. A. Le Dez, (2019), "Tactique Cyber, le combat numérique". Paris: Economica.
3. Armée de Terre, (2008), *Tactique Générale*. Paris: Economica, 28-32.
4. A.M. Turing, (1950), Computing machinery and intelligence. *Mind* LIX (236), 433-460.
5. A.M. Turing, (1936), On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42: 230–265.
6. R. Guyonneau, (2019), Extension of the machine's realm: a brief insight into Artificial Intelligence and Cyberspace. *The Cyber Defense Review*. <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1880459/extension-of-the-machines-realm-a-brief-insight-into-artificial-intelligence-an/>
7. T. Rid, and B. Buchanan, (2015), Attributing Cyber Attacks. *The Journal of Strategic Studies* 38 (1-2), 4-37.
8. Silver, S., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K., Hassabis, D. A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play. *Science* 362(6419), 1140-1144 (2018).
9. A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay and D. Mukhopadhyay, (2018), "Adversarial Attacks and Defences: A Survey". *ACM Comput. Serv.*
10. J.M. Carmena, M.A. Lebedev, R.E. Crist, J.E. O'Doherty, D.M. Santucci, D.F. Dimitrov, P.G. Patil, C.S. Henriquez and M.A.L. Nicolelis, (2003), Learning to control a brain-machine interface for reaching and grasping by primates. *PLoS Biology* 1(2), e42.
11. J. Von Neumann, (1958), *The computer and the brain*. Yale University Press.
12. Y. LeCun, Y. Bengio and G. Hinton, (2015), Deep Learning. *Nature* 521, 436-444.
13. S. Ullman, (2019), Using neuroscience to develop artificial intelligence. *Science* 363 (6428), 692-693.



# The Post-GIG Era: From Network Security to Mission Assurance

---

Dr. Kamal Jabbour, ST

## ABSTRACT

**T**he shortcomings of the Global Information Grid (GIG) may be traced to a disconnect between cyber policy and technology, and an illusion that cyber defense contributes somehow to mission assurance. Therefore, it is necessary to look past the GIG to a future of affordable access and mission assurance. Prescriptive cyber policies have impeded the mission, as the compliance approach to security led to indiscriminate application of monitor-detect-react constructs to Information Technology (IT) systems regardless of criticality.

In this paper, we present a paradigm shift from cybersecurity through network defense to mission assurance through information assurance. We shift our emphasis from the illusion of building persistent security out of trusted components to the imperative of composing timely assurance out of untrusted components. We distinguish between national security missions and office automation applications and acknowledge the different risk calculus for missile defense versus online commerce. We advocate a shift away from the GIG towards commercial cloud solutions across all phases of the information life cycle, mathematical specification of mission requirements, and implementation validation through operationally realistic testing.

We propose a three-pronged strategy to assure national security missions in a contested cyber environment, focusing separately on legacy systems, current systems, and future systems. Each category brings unique technological challenges, with little commonality within the three categories. We advocate Tactics, Techniques, and Procedures (TTP) wherever applicable, commercial materiel solutions where a TTP-only mitigation falls short, and revolutionary Science and Technology (S&T) where TTP and commercial solutions prove insufficient.

*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. Kamal T. Jabbour**, a member of the scientific and technical cadre of senior executives, is senior scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry. Dr. Jabbour is an avid distance runner and has completed marathons in all 50 states.

## PROBLEM STATEMENT

The myth of intrusion detection dates to the 1980s<sup>[1]</sup> and has led gradually to a group think culture intent on monitoring networks and computers in the hope of detecting and responding to intrusions in a timely manner.

The introduction of the International Business Machines (IBM) 360 family of computers in the 1960s brought about memory management, dynamic address translation, and resource sharing and, with these advancements, the genesis of time-shared operating systems.<sup>[2]</sup> In a 1972 USAF report, James Anderson of the Electronic Systems Division at Hanscom Field, MA, singled out resource sharing as a security concern. Anderson dismissed the insertion of security software between an application and the operating system as resource-intensive and ineffective<sup>[3]</sup>.

Two centuries earlier, Scottish philosopher David Hume introduced the induction problem in his 1739 work, “A Treatise of Human Nature”.<sup>[4]</sup> Hume stated that “there can be no demonstrative arguments to prove that those instances of which we have had no experience resemble those of which we have had experience,” a prophecy of the failure of every cyber defense that relies on the past to secure the future.

The Internet owes a great deal to Robert Kahn and Vint Cerf for developing the TCP/IP protocols<sup>[5]</sup> on the firm foundation of layering, where Layer N provides services to a higher Layer N+1, and functions at Layer N+1 allow recovery from failures at a lower Layer N. This foundation implies that packet monitoring at the lower Network Layer cannot detect, let alone defeat, cyber-attacks at the higher Application Layer.

Hume, Anderson, and Kahn provide the necessary mathematics to assess the effectiveness of a cyber security tool. If a tool projects the past onto the future, if it requires resource sharing from the system it seeks to defend, or if it operates at the wrong layer, then we assess axiomatically that the tool will fail its intended purpose.



We applied the Hume-Anderson-Kahn axiom to explain the failure of firewalls, cross-domain solutions, guards, intrusion detection systems (IDS), intrusion prevention systems (IPS), virus scanners, malware detection, deep packet inspection, network monitoring, audit logs, black-listing, white listing, attestation, insider threat detection, normal traffic characterization, abnormal traffic detection, access control lists, honey pots, to name a few. Ironically, a cyber security gadget that violates one of the Hume-Anderson-Kahn laws often violates all three.

## BACKGROUND

### *Layered Architectures*

The specification of the Internet Protocol (IP) in the 1970s that we attribute to Robert Kahn and Vint Cerf, and the publication of the International Standards Organization (ISO) Open Systems Interface (OSI) reference architecture, set the stage for a layered implementation of the ARPANET, and subsequently the Internet. At its most fundamental level, the ISO OSI reference architecture specifies that a problem at Layer N can only be fixed at Layer N+1.

The seven layers of the ISO OSI reference architecture map loosely to the five TCP/IP layers:

7. Application Layer	5. Application Layer
6. Presentation Layer	-
5. Session Layer	-
4. Transport Layer	4. Transmission Control Protocol (TCP) Layer
3. Network Layer	3. Internet Protocol (IP) Layer
2. Data Link Layer	2. Media Access Control (MAC) Layer
1. Physical Layer	1. Physical Layer

Each of the seven ISO OSI layers seeks to overcome limitations of lower layers while providing services to upper layers:

- 7. Application Layer:** user and process applications
- 6. Presentation Layer:** data presentation, including encryption and compression
- 5. Session Layer:** session management, login/logout, authentication
- 4. Transport Layer:** host-to-host data transport
- 3. Network Layer:** routing and accounting
- 2. Data Link Layer:** packetization, error detection and retransmission, error correction
- 1. Physical Layer:** raw bit stream plus noise and errors

A similar deconstruction shows the seven layers of a computer architecture:

7. **Application Layer:** user and process applications
6. **High-Level Languages Layer:** 1-to-N constructs, compilers, interpreters
5. **Assembly Language Layer:** 1-to-1 mnemonics, macros
4. **Operating System Layer:** input-output, memory management, resource sharing
3. **Machine Language Layer:** architecture
2. **Microprogramming Layer:** firmware, maps architecture onto hardware
1. **Digital Logic Layer:** hardware, gates

In 1972, Anderson recognized that security problems at the Application Layer (Layer 7) from resource sharing at the Operating System Layer (Layer 4) could not be fixed by inserting tools between the two layers. Such tools exerted a significant performance penalty and failed to mitigate against a skilled adversary. In his assessment, Anderson foretold the failure of host-based security systems.

Similarly, any attempt to defend against security threats at the Application Layer by deploying solutions at the Network Layer violates the fundamental premise of layering on which Kahn built TCP/IP and is destined to fail. Thus, deep packet inspection of network traffic for intrusion detection and prevention, as well as filters and firewalls at Layer 3, fail to detect—let alone prevent—covert channels at Layer 7.

Layering introduces a fundamental asymmetry that frustrates security novices seeking the cyber high ground, or the race to the bottom, suggesting that the process that owns Layer 1 controls the environment. This suggestion is partially true: a Byzantine hardware failure at Layer 1 increases the risk of application failure at Layer 7, but well-behaved hardware does not assure application success in the presence of an ill-behaved operating system.

For mission assurance, we interpret this layering asymmetry differently: a cyber-attack that compromises the hardware increases the risk of mission failure, but a secure processor does not assure mission success against attacks on the intermediate layers.

### *Efficiency versus Effectiveness*

Artificial Intelligence (AI), Machine Learning (ML), Big Data (BD), Command and Control (C2), Behavior Modeling (BM), Automation and Autonomy (AA), promise to increase the efficiency of well-behaved processes, but have no impact on the effectiveness of these processes. In other words, applying AI-ML-BD-C2-BM-AA to a signature-base IDS will not improve its ability to detect a zero-day exploit, but rather increases the rate and frequency of IDS failure.

### *User Training*

No discussion of the failure of cyber defense is complete without an honorable mention of the poster child of cyber failures; user training. From inserting thumb drives and clicking on

hyperlinks, to opening attachments and phishing emails, the proverbial dumb user has fueled an insatiable appetite to regulate and train. Notwithstanding the effective technology solutions that can reduce the mission risks from dumb users and spare the dumb user the elusive pursuit of cyber expertise, policymakers demand compliance and threaten discipline.

## TOOLS AND TECHNIQUES

### *Risk Metric*

The National Institute of Standards and Technology (NIST) defines the risk to information systems as a function of the likelihood that a vulnerability exists; the threat necessary to exploit the vulnerability, and; the effect resulting from a successful exploitation:<sup>[6]</sup>

$$\text{Risk} = \text{P}(\text{vulnerability}) \times \text{P}(\text{threat} \mid \text{vulnerability}) \times \text{Effect}$$

We interchangeably use the terms effect, impact, and consequence.

Our vulnerability assessment of various systems led us to define three classes of potential vulnerability:<sup>[7]</sup>

- i. architecture vulnerability:** resource sharing and Byzantine behavior
- ii. specification vulnerability:** protocols and Modes of Employment (MOE)
- iii. implementation vulnerability:** hardware, software, and configuration.

Unfortunately, current vulnerability scanning tools have the narrow scope of less than 10 percent of the vulnerability surface, as they look primarily at configuration vulnerability. The effectiveness of these tools over that scope is another matter (Hint: zero). Yet these tools increase the risk to these systems by increasing their attack surface.

We break the cyber threat<sup>[8]</sup> into three components:

- i. capability:** time, talent, and resources necessary to exploit a vulnerability
- ii. access:** physical, network, wireless
- iii. intent:** we assume malicious intent.

The conditional nature of adversaries threatening to exploit a potential vulnerability implies that there is no threat without vulnerability. This is a fundamental concept that shows how ineffective it is to focus narrowly on defeating threats without taking vulnerability into consideration.

We focus on degree and duration as the two aspects of successful exploitation of a vulnerability. We consider disruption to be a temporary and partial affect; denial a temporary but total effect; degradation a permanent but partial effect; and destruction a permanent total effect.

The duration of adverse effects of a cyber-attack is a function of mission duration. When we measure the duration of many critical functions in seconds, a monitor-detect-respond-recover approach operates inevitably in recovering from mission failure.

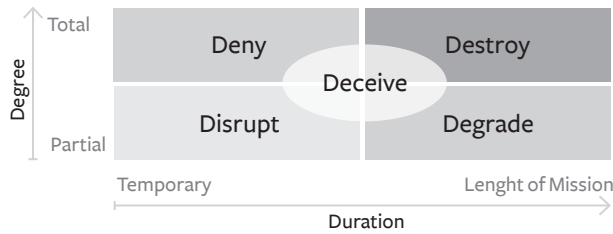


Figure 1. Effects of a cyber-attack

**Scope, Effectiveness, and Risk**

Prior to mandating a new procedure or implementing a new policy, it is imperative to assess its utility in terms of scope, effectiveness, and risk. Such assessment applies equally to host-based monitoring tools, manned activities, and compliance enforcement.

An assessment of a security artifact begins by defining its scope—the percentage of the attack surface it seeks to cover. For example, deep packet inspection on a network carrying 70 percent encrypted traffic has a scope of 30 percent. Similarly, a Windows vulnerability assessment scan against an aircraft has a scope of zero, and a penetration testing scan against a satellite will fail to detect an architecture vulnerability.

Given the scope of a cybersecurity gadget, measuring its effectiveness allows computing an estimate of its utility as the product of scope times effectiveness. Unfortunately, when a tool violates Hume-Anderson-Kahn, its effectiveness against an advanced threat computes to zero, giving zero utility regardless of breadth of scope.

Compliance enforcement requires selecting security controls deemed applicable to a mission, implementing these controls, then testing these controls. If a chosen security control relies on the past to secure the future in violation of Hume, or if its implementation requires sharing resources with the system under test in violation of Anderson, or if the control operates at the wrong layer in violation of Kahn, then compliance enforcement turns an ineffective compliance vehicle into an attack vector.

**Information Assurance Tenets**

The three tenets of information assurance are confidentiality, integrity, and availability. The Advanced Persistent Threat (APT) targets information confidentiality by hiding for an extended period of time on a target and copying information. Destructive attacks do not hide; they target information availability by destroying information and computers. Access-less attacks, such as Border Gateway Protocol (BGP) exploits, target information integrity by hijacking traffic and injecting incorrect information.

The most challenging attacks are those that target information integrity. Byzantine fault analysis provides the science to assess system vulnerability to integrity attacks. A Byzantine fault creates the same effect regardless of intentional or accidental cause.<sup>[9]</sup> In simple words, Byzantine fault analysis looks at the effect when a computer lies, not when a computer dies.

### *Information Lifecycle*

The evolution of military systems from Government Off-The-Shelf (GOTS) to Commercial Off-The-Shelf (COTS), the outsourcing of integrated circuit fabrication and software development, and the transition from dedicated transmission lines to commercially-procured leased circuits, have increased the dependence on a diverse supply chain and a commensurate risk of supply chain manipulation. Besides hardware we did not build, software we did not write, and circuits we did not lay, the shift from GOTS to COTS includes protocols we did not specify, users we did not train properly, and operators we did not educate adequately.

The DoD has neither the will nor the ability to reverse the shift from GOTS to COTS. Therefore, it is unrealistic to expect that the security of the supply chain will improve with new ways to monitor-detect-respond to security failures, leaving us with no choice other than assuring our missions with untrusted components—hardware, software, networks, protocols, users, and operators.

Composing mission assurance with untrusted components necessitates assuring information—the only asset that we own and control—across the six phases of the information lifecycle:<sup>[10]</sup>

- i. Information generation
- ii. Information processing
- iii. Information transmission
- iv. Information storage
- v. Information consumption
- vi. Information destruction

Disciplined cyber vulnerability mitigation must assure information flows throughout a mission across the entire information lifecycle.

## **OUR PROPOSED SOLUTION**

### *Vision, Mission, and Strategy*

We envision an enduring assurance, a cyberspace with no vulnerability. We seek to assure critical missions through a paradigm shift from computer security to information assurance by creating a cyber domain that assures information across all stages of conflict, leading to friendly missions with no vulnerability in peacetime, denying the impact of cyber threat in escalation, and exploiting at will adversary missions in wartime.

Our strategy uses Byzantine fault analysis to develop dual-purpose Science and Technology (S&T) to create provable mission assurance through disaggregation and composition of untrusted components, and to disproportionately increase the cost to the cyber threat, while holding at risk adversary missions.

The big building blocks of this vision rely on breaking down information risk into its stochastic components of vulnerability, threat, and impact. This breakdown provides threat independence through Byzantine fault analysis. For current and legacy systems, we propose mission assurance through prioritization of Mission Essential Functions (MEF), cyber dependence, vulnerability assessment, and vulnerability mitigation.

Enduring assurance requires designing future missions by mathematical specification and formal verification and implementing information disaggregation and just-in-time mission composition of untrusted components into assured missions with physics-based security. We advocate cyber deterrence<sup>[11]</sup> through superiority at a time and place of our choosing with intelligent cyber agents that operate on a continuum from direct command-and-control through automation to autonomy. Our vision of enduring assurance requires developing a cyber workforce through education on the science of information assurance and training on the art of cyber warfare and developing a scientifically relevant cyber doctrine<sup>[12]</sup>.

## **IMPLEMENTATION ROADMAP**

### *Mission assurance of legacy and current systems*

MEF cyber dependence requires a disciplined vulnerability assessment of the architecture, specification, and implementation, followed by a systematic vulnerability mitigation through TTP, materiel solutions where available, and S&T in the absence of commercial solutions.

Byzantine fault analysis focuses on information integrity and enables MEF migration into public clouds in virtual machines, direct code translation, or mission revalidation and mathematical synthesis.

We propose the following phased implementation of mission assurance of legacy and current systems:

- i. Adhering to Hume-Anderson-Kahn by removing the attack vectors against national security missions brought about by RMF, especially monitoring, intrusion detection, virus scanning, audit logging, remote administration, and remote configuration.
- ii. Transitioning office automation applications into a Software-as-a-Service (SaaS) public cloud such as Microsoft and Google.
- iii. Porting the network components of national security missions into an Infrastructure-as-a-Service (IaaS) public cloud such as Amazon and IBM.
- iv. Enforcing zero-trust operation such that no user and no computer may adversely impact a critical mission, regardless whether the trigger is intentional or accidental.
- v. Implementing Layer 8, the Mission Layer, to permit recovery from failures or attacks against Layer 7, the Application Layer.
- vi. Introducing diversity and heterogeneity in the hardware and software to hedge against mono-culture failures.

### *Inventing the future: S&T for future missions and systems*

Information assurance across the information lifecycle holds the key to mission assurance with untrusted components. As we design future missions, we must perform a trade-off between integrity and availability, as we seek execution validation for a trusted outcome.

Assuring future missions requires mathematical specification of the requirements at the far left of the acquisition lifecycle, then formal verification and testing of the implementation throughout the lifecycle. Rather than seeking resilience—recovery after every failure—we seek antifragility through information disaggregation in a public cloud<sup>[13]</sup>.

To assure against supply chain threats, we must pursue system design for testability, and just-in-time mission composition. We advocate the split fabrication of integrated circuits to reduce the risk of hardware backdoors, and automatic code generation against software backdoors. Finally, we have demonstrated the utility of physics-based assurance through Physically-Unclonable Functions (PUF), ternary encryption, and practically-homomorphic encryption.

### *Cyber superiority at a time and place of our choosing*

The later stages of conflict leading to large scale combat operations necessitate deploying a wartime reserve mode Layer 8 for contingency operations, atop a dedicated IPvMil network implementation. We envisage a three-stage development of IPvMIL to demonstrate:

- (1) Cooperative deployment on Blue assets with uncontested employment,
- (2) Cooperative deployment on Blue assets and Gray commons, with contested employment, and
- (3) Non-cooperative deployment on Blue assets, Gray commons, and Red targets, with contested employment.

The natural progression from mathematical requirement specification and formal implementation verification is polymorphic contingency mission execution on higher-order number systems (somewhere between binary and quantum), assuring mathematical orthogonality to adversary threats.

While AI-ML-BD-C2-BM-AA serve no purpose in DCO, these technologies hold great promise for Offensive Cyber Operations (OCO) leading to cyber superiority. We advocate the development and deployment of intelligent agents capable of operating along the continuum of direct command and control (C2), automation, and autonomy.

We propose theater-scale war games informed by intelligence on adversary capability, free from the restrictions of our interpretation of adversary intent, or the illusion that defenders can detect and respond to a cyberattack in a mission-relevant timeframe. Finally, the DoD must rewrite its cyber warfare doctrine from “the way we wished it were” to “the way it actually is.” Cyber warfare must be informed by technology and enforced by technology.

### ***Risk Analysis***

The Defense Digital Service (DDS) is conducting an experiment that leverages industry best practices in computing and networking to assure selected IT applications. The post-GIG vision builds on the DDS experiment and extends it from IT applications to national security missions. We are confident that we can compose timely mission assurance from untrusted components, and assure access, integrity, and affordability, and, in the process, demonstrate that cybersecurity is neither necessary nor sufficient for mission assurance.

### **CONCLUSION**

We propose a paradigm shift from cybersecurity through network defense, to mission assurance through information assurance, focusing primarily on assuring national security missions across the stages of conflict. We leverage age-old truths to demonstrate that cyber security is neither necessary nor sufficient for mission assurance and we recommend composing timely assurance out of untrusted components, and a shift towards commercial cloud solution.🛡️



## NOTES

1. Dorothy E. Denning, “An Intrusion Detection Model”, IEEE Transactions on Software Engineering, vol. SE-13, no. 2, February 1987, 222-232.
2. “System 360 – From Computers to Computer Systems”, International Business Machines (IBM), <https://www.ibm.com/ibm/history/ibm100/us/en/icons/system360/>.
3. James P. Anderson, “Computer Security Technology Planning Study”, HQ Electronic Systems Division, L.G. Hanscom Field, Bedford, MA, October 1972.
4. David Hume, “A Treatise of Human Nature”, 1739.
5. Vinton G. Cerf and Robert E. Kahn, “A Protocol for Packet Network Intercommunication”, IEEE Transactions on Communications, Vol. COM-22, May 1974.
6. “Managing Information Security Risks”, National Institute of Standards and Technology, SP 800-39, March 2011.
7. Dr Kamal Jabbour and Maj Jenny Poisson, “Cyber Risk Assessment in Distributed Information Systems”, Cyber Defense Review, Spring 2016, 79-100.
8. Dr Kamal Jabbour and Dr Erich Devendorf, “Cyber Threat Characterization”, Cyber Defense Review, Fall 2017, 79-93.
9. Fred B. Schneider, “Blueprint for a Science of Cybersecurity”, The Next Wave, vol 19, no 2, 2012, 47-57.
10. Dr Kamal Jabbour and Dr Sarah Muccio, “The Science of Mission Assurance”, Journal of Strategic Security, vol 4, no. 2, Summer 2011, 61-74.
11. Dr Kamal Jabbour and E. Paul Ratazzi, “Does the United States Need a New Model for Cyber Deterrence?” Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century, Edited by Adam B. Lowther, 2012, 33-45.
12. Dr Kamal Jabbour, “The Time has Come for the Bachelor of Science in Cyber Engineering”, High Frontier: The Journal for Space and Cyberspace Professionals, vol 6, no 4, 2010, 20–23.
13. Erich Devendorf, Kayla Zelif and Kamal Jabbour, “Characterization of Antifragility in Cyber Systems Using a Susceptibility Metric”, ASME 36th Computers and Information in Engineering Conference, August 2016.



# THE CYBER DEFENSE REVIEW

◆ RESEARCH NOTE ◆



# Future Geospatial Disinformation Campaigns

---

Lieutenant Colonel David M. Beskow

Kathleen M. Carley, Ph.D.

## ABSTRACT

Social media is increasingly used as a source of data to provide situational awareness and decision support tools for world events including sporting events, democratic elections, and natural disasters. As this data is increasingly used in these scenarios, it also becomes vulnerable to manipulation. This manipulation can take several forms which have been variously explored. This paper will highlight the vulnerability of future manipulation of social media geospatial data.

## I. INTRODUCTION

As social media has become the medium through which many people consume news and information<sup>[7]</sup>, it has also become the marketplace for beliefs and ideas. This marketplace has recently been manipulated by highly organized disinformation campaigns by both state and non-state actors.<sup>[3]</sup> These actions generally involve manipulation of the actual network or of the information in order to gain an unfair advantage in the information marketplace.

While these disinformation campaigns are emerging to manipulate social media platforms, the same platforms and associated data are used by a variety of organizations to help understand world events. Social media data is used by financial companies<sup>[4]</sup>, national security organizations<sup>[1]</sup>, emergency response organizations<sup>[6]</sup>, news outlets<sup>[5]</sup>, and political organizations<sup>[2]</sup> to provide situational awareness and decision support tools. The known use of this data to support decision making in these events will likely increase the incentives to launch disinformation campaigns to manipulate decision making or simply to sow discord. To date, there has not been a widespread, publicized attempt to manipulate the geographic dimension of this data. This paper will highlight the future possibility of this by expanding on the innocent manipulation of this data by a Twitter bot hobbyist.

*Lt. Col. David M. Beskow's contribution is a work of the U.S. Government and is not subject to copyright protection in the United States.*

*Foreign copyrights may apply.*

*© 2019 Dr. Kathleen M. Carley*



**Lt. Col. David Beskow**, U.S. Army, is a PhD candidate in the School of Computer Science at Carnegie Mellon University. During his career, Beskow served as an infantry leader in the 82nd Airborne Division and the 4th Infantry Division. As an FA49 operations research and systems analyst (ORSA), Beskow served as an assistant professor at West Point and as an ORSA analyst at the U.S. Army Intelligence and Security Command. Beskow's current research develops machine learning algorithms to detect and characterize online bots and the disinformation campaigns they inhabit.

## II. BACKGROUND

Our team has been monitoring Twitter and other social media outlets for NATO-related conversations for several months leading up to NATO Trident Juncture 2018 Exercise, held in October and November 2018 in Scandinavia. As the largest military exercise ever held in Norway, we expected NATO-related disinformation campaigns from Russia and Russian proxies to target this event.

While monitoring the NATO-related conversation, we periodically visualized the geospatial nature of the Twitter conversation in Scandinavia. During one such investigation, we found that a bot hobbyist in Finland created a bot that tweeted the Finnish numbers while geo-locating these tweets in a uniform distribution across the longitude and latitude of the bounding box of Finland. This bot was discovered in the geo-spatial visualization provided in Figure 1. In this figure, the two-dimensional, uniform distribution across the bounding box of Finland is clearly evident.

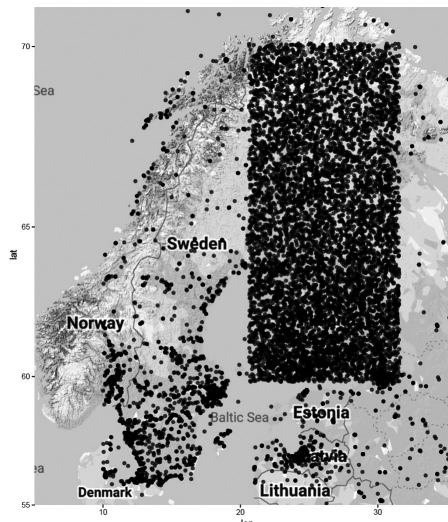


Figure 1. Map showing Finnish bot designed to locate tweets uniformly in the bounding box of Finland



**Kathleen M. Carley, PhD**, is a professor of societal computing in the School of Computer Science at Carnegie Mellon University, an IEEE Fellow, the director of the Center for Computational Analysis of Social and Organizational Systems (CASOS), and the CEO of Netanomics. She is the 2011 winner of the Simmel Award from the International Network for Social Network Analysis and the 2018 winner of the USGA Academic Award from GEOINT.

This bot produces a tweet once every minute that slowly goes through positive integers in the Finnish language. It has been tweeting since October 2014 and has produced 1.69 million tweets (we captured 6,734 of these in Figure 1). The very simple Python function used by this account was available on Github and is provided in Listing 1.1.

```

1 def random_point_in(bbox):
2     '''Given a bounding box of (swlat, swlon, nelat, nelon),
3     return random (lat, lon)'''
4     lat = random.uniform(bbox[0], bbox[2])
5     lon = random.uniform(bbox[1], bbox[3])
6     return (lat, lon)

```

Listing 1.1. Python Code from Finnish Bot

### III. POTENTIAL FOR MALICIOUS EFFECTS

Although this account has good-natured intentions, the power of this geospatial data manipulation is clearly evident in Figure 1. In this case it was easy to clean the data since the tweets were generated by a single account in an easily recognizable rectangular pattern. A determined actor, however, could activate a dormant *bot army* to generate Tweets, and geo-locate them in a manner to either

1. Carpet the area in spatial tweets to create enough noise to mask the underlying signal of interest (i.e. true calls for help in natural disaster), rendering the underlying data useless for situational awareness or decision support (most likely).
2. Create a fake social event or fake social signal to sow discord or enable an elaborate deception operation (most dangerous).

If we consider this manipulation a type of *offensive information operation*, then we need to consider the resulting *defensive information operation*. In this case, data scientists at social media companies and government agencies would attempt to identify all accounts and content associated with the offensive disinformation operation. These efforts would seek to find any pattern in the attack, and then leverage machine learning

algorithms to identify malicious accounts at scale, similar to current methods that identify traditional bots<sup>[3]</sup>. They would look for any patterns in the account features (similar names, descriptions, language settings) or account activity (similar language, content, temporal correlation, etc) or geospatial distribution (easily identifiable distributions, such as the Finnish bot).

Therefore, given the known techniques used to *clean* the data, for an offensive information operation to achieve full success with geospatial disinformation, it would need to have the following characteristics:

- ◆ Leverage a large number of accounts (i.e. a *bot army*) that appear to be local to the target area (i.e. have reasonable language, time zone, and life patterns).
- ◆ Leverage data sampling and varied random distributions to create an elaborate and realistic geospatial pattern.
- ◆ Create content that blends easily with local conversation.
- ◆ Duration must be just long enough to achieve success, and, after, with accounts would blend back into the conversation.

The desired end state for an offensive geospatial disinformation operation is to cause confusion and operational paralysis, while the offensive actor maintains access to most of their *bot army*.

Note that a sophisticated actor is not confined to geometric shapes or even to simple random distributions. They could use a variety of methods to generate synthetic geo-spatial coordinates that approximate the true social media geospatial distribution. They can create these patterns by producing Gaussian *jitter* around a sample of real data (see Figure 2a) or by sampling a multivariate uniform distribution through a population density raster as illustrated in Figure 2b. Either of these would accomplish the same effect, namely creating seemingly genuine social media geo-coordinates with which they can execute their geospatial disinformation campaign.

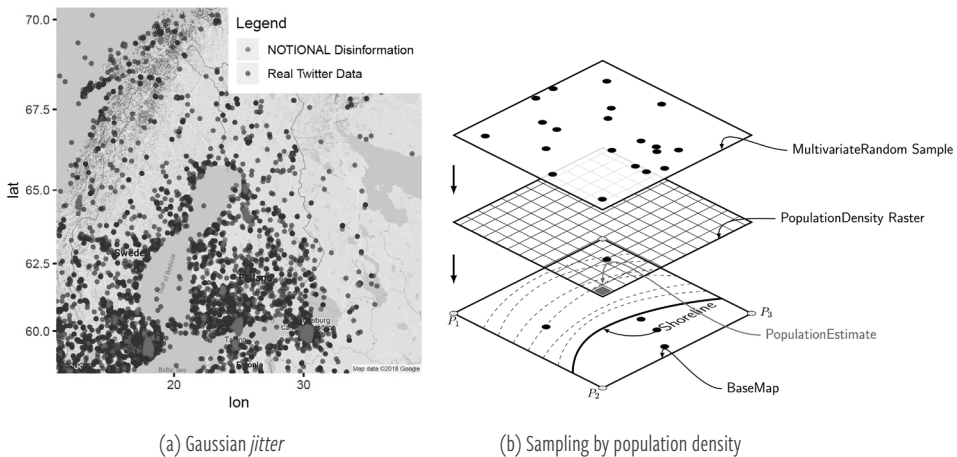


Figure 2. Two methods that could be used to create synthetic geospatial coordinates that approximate genuine social media geospatial distributions



Given these requirements, these inevitable geospatial information operations will require a degree of sophistication to achieve operational success. With the requisite degree of sophistication and planning, these operations would be difficult to defend and would create operational confusion and possibly, paralysis. The eventual result could be that specific social media platforms and data may be rendered useless for situational awareness and decision making for key leaders in finance, emergency response, and national security.

#### IV. NOTIONAL GEOSPATIAL DISINFORMATION OPERATION

In this section we will illustrate the potential danger of geospatial disinformation campaigns. We will do this with a **NOTIONAL** disinformation campaign inserted into the real-world data associated with Hurricane Michael, a Category 4 hurricane which struck the Gulf Coast in October 2018. All synthetic data was inserted after the fact; our team did not create or manipulate Twitter to create this notional scenario.

In this scenario, we create a notional actor who wants to create confusion and chaos around Tyndall Air Force Base (AFB) during the hurricane and use this chaos to gain unauthorized access to the base for malicious or espionage purposes. Given that the base was in the eye of the storm, all but essential personnel were evacuated from the base, and therefore very few social media posts were emanating from Tyndall AFB during and immediately after the storm. To create the chaos, our notional actor posts numerous fake cries for help on Twitter, all geo-spatially located inside Tyndall AFB cantonment area. The notional actor would then attempt to infiltrate the base when numerous off-base first responders attempt to gain access to the base to respond to these false alarms.

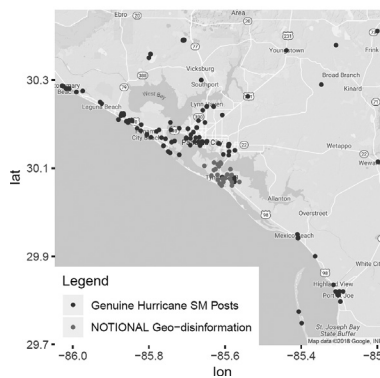


Figure 3. Notional Example of Geospatial Disinformation

In Figure 3, our team has inserted *notional* data (red) on top of the genuine hurricane related Twitter posts (blue). To create the simulated geospatial disinformation below, our team created a multivariate random normal distribution centered on Tyndall AFB and used a point-in-polygon algorithm to remove all points that were in the water. The notional actor would then attach fake calls for help to these geographic coordinates and post them in the form of a tweet or other social media post. To do this, the malicious actor could create their own content, or more likely mimic or copy the real calls for help already associated with the natural disaster.

This seemingly real surge in calls for help from the Tyndall AFB would undoubtedly cause multiple off-base first responders attempt to get base access to rescue the supposed victims. The malicious actor could then use the chaos that ensues to insert their own agents onto Tyndall AFB to sabotage or conduct espionage operations. In the notional example above, we have illustrated a targeted, geospatial, disinformation operation associated with a natural disaster. These type of information operations could be deployed in conjunction with a terrorist attack, a humanitarian crisis, or combat operations. In all cases the geospatial disinformation would create confusion and chaos, alter decision making, and in the end, render the underlying data source unreliable and unusable.

### **V. CONCLUSIONS**

In this paper, we have highlighted how the manipulation of geospatial information in social bot disinformation campaigns can deceive and disrupt organizations who use that data for situational awareness and decision support. These geospatial disinformation campaigns may be simply trying to hide the signal in noise, or they may be trying to support an elaborate deception operation. Regardless, the initial effect will be confusion and operational paralysis. Long term strategic effects could include degraded value for large open source data (i.e. neutralization of *big data* advantage).🛡️

### **DISCLAIMER**

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

### **ACKNOWLEDGMENT**

This work was supported in part by the Office of Naval Research (ONR) Multidisciplinary University Research Initiative Award N000141812108, Office of Naval Research Minerva Awards N00014-13-1-0835/N00014-16-1-2324, and the Center for Computational Analysis of Social and Organization Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the ONR or the U.S. government.

## NOTES

1. M. Benigni and K. M. Carley (2016), From tweets to intelligence: Understanding the islamic jihad supporting community on twitter, In *Social, Cultural, and Behavioral Modeling: 9th International Conference, SBP-BRiMS 2016, Washington, DC, USA, June 28-July 1, 2016, Proceedings 9*, Springer, 346– 355.
2. W. L. Bennett and A. Segerberg (2012), The logic of connective action: Digital media and the personalization of contentious politics, *Information, Communication & Society* 15(5), 739–768.
3. D. Beskow and K. M. Carley (2018), Introducing bothunter: A tiered approach to detection and characterizing automated activity on twitter, In H. Bisgin, A. Hyder, C. Dancy, and R. Thomson (Eds.), *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*. Springer.
4. M. J. Culnan, P. J. McHugh, and J. I. Zubillaga (2010), How large us companies can use twitter and other social media to gain business value, *MIS Quarterly Executive* 9(4).
5. R. Goolsby, (2010), Social media as crisis platform: The future of community maps/crisis maps, *ACM Transactions on Intelligent Systems and Technology (TIST)* 1(1), 7.
6. M. Latonero and I. Shklovski (2013), Emergency management, twitter, and social media evangelism. In *Using Social and Information Technologies for Disaster and Crisis Management*, IGI Global, 196–212.



# THE CYBER DEFENSE REVIEW

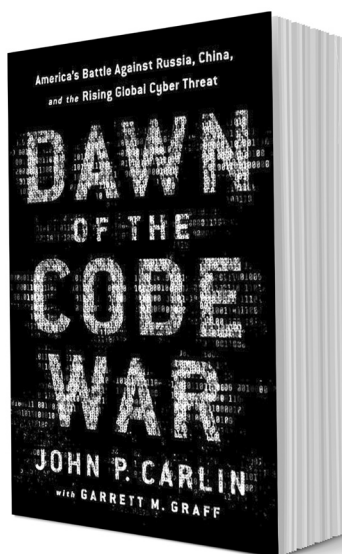
◆ BOOK REVIEW ◆



# Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat

by John P. Carlin

Reviewed by  
Philip C. Shackelford



## EXECUTIVE SUMMARY

“Winning the Code War first requires recognizing that the war has already begun.”

With this final sentence in the Epilogue, John Carlin, former Assistant Attorney General for National Security, summarizes the central thrust of his book—telling the story of how “criminals, terrorists, and spies made themselves at home on a global network that was never designed with safety and security in mind” and detailing the ways in which the United States government, prosecutors, the FBI, and our allies around the world have spent twenty-five years “playing catch-up.” *Dawn of the Code War* is part memoir, as Carlin himself was intimately involved with many of the struggles he describes; part history that chronicles high points in the development of cyber threats since the beginning of the Internet; and part warning as Carline reminds us that we have “built our modern society on top of fragile technology, with far too little thought as to the creativity of our adversaries.” Carlin does not rest his argument solely on the context of his direct involvement in the “Code War,” but supports his narrative with a robust combination of public media sources and government and corporate documents and press releases. Carlin covers technical details in a manner that allows the reader to have a broad understanding of developments without bogging the text down in unnecessary minutiae. This result is a novice-friendly approach that promotes the “big picture” perspective Carlin seems to favor. Carlin succeeds in “demystifying” the realm of cyber war, raising awareness of the threat landscape, and highlighting thought-provoking questions about our dependence on the Internet and approach to cyber threats.

© 2019 Philip Shackelford



**Philip Shackelford** is the Library Director at South Arkansas Community College in El Dorado, Arkansas. He currently serves as Awards Chair for the Arkansas Library Association as well as Secretary of ARKLink, the Arkansas Academic Libraries Consortium. His historical research focuses on the Cold War history of the U.S. Air Force, the Air Force Security Service, and the history of intelligence and national security during the early Cold War. His recent article “Fighting for Air: The Struggle for Air Force COMINT, 1945-1952” was published in the *U.S. Military History Review*, and Philip continues to write, research, review, and publish in this area. Philip holds a Master’s degree in History and a Master’s degree in Library and Information Science, both from Kent State University in Kent, Ohio.

## REVIEW

A central thread throughout *Dawn of the Code War* relates to cybercrime and law enforcement, and the difficulty of figuring out how to “impose the laws and rules of the physical world” onto a virtual place “you can’t see but you know is there.” One issue is determining the financial damage to companies, governments, and individuals because of cybercrime. Another is understanding how to bring existing laws and legal standards to bear on a category of criminal activity that Carlin believes is still in its infancy and that, particularly early on, did not have direct, applicable legal parallels. Indeed, some of the earliest examples of cybercrime were legally defined as making obscene or harassing telephone calls or breaking and entering. The U.S. government did not yet possess an applicable framework for prosecuting cybercrime. Such issues conflicted with the popular belief that the Internet was a free and open tool for education, discovery, and expression. At the time, few could imagine the extent to which the Internet would become integrated with so many aspects of our daily lives. This dependence on the Internet amplifies the risk at hand—Carlin uses the analogy that we are “living in an online house of straw, yet even as the wolf approaches the door, not only are we not seeking shelter in a stronger house, we’re continuing to cram ever more stuff into our straw house.”

Cybercrime did not remain limited to innocent, prankster-like activity for long, as the Internet soon became a hub for criminality and malicious attacks. Cybercrime and cyberwar continue to defy traditional definition. They are a “complicated, multidimensional, international” tension that requires resources and attention from both government and private sectors. The Code War does not involve a single set of opposing actors or ideologies but is characterized by myriad and anonymous adversaries and vulnerabilities.



Carlin identifies three distinct “epochs” of evolving cyberthreats and believes that we are moving into a fourth. First, he emphasizes China and its practice of engaging in economic espionage, stealing government and corporate secrets. His second “epoch” begins in the late 2000s, when Iran began conducting destructive digital attacks, including an attempt to assassinate the Saudi ambassador in a Washington, D.C. restaurant, followed by digital attacks on the Wall Street financial sector and a Las Vegas casino owner. Third, North Korea fused digital attacks with social media awareness to amplify the impact of their attack. Finally, Carlin believes that we are seeing the emergence of a fourth “epoch” in which bad actors—both nation-states and non-state actors—combine cyberattacks with real-world “kinetic” attacks. Examples of this include targeting power grids, hospitals, and the Internet of Things.

Not only has the rise of the Internet exposed modern society to “complex and unprecedented” threats, but Carlin points out that it has fundamentally blurred our understanding of the world as well, in six different ways. Specifically, the Internet has blurred the lines between peace and war, between public and private, the nation-state vs. the individual, physical vs. virtual, distinctions between borders, and obscured our understanding of what is “secret” and what is “critical infrastructure.” These obfuscations have profound implications as government officials and lawmakers struggle with an inadequate vocabulary for describing and framing attacks. What constitutes an act of war? What is “critical infrastructure?” What does an appropriate and proportional response look like?

Hence comes Carlin’s word of warning—his position that our approach as a nation and society remains “inadequate.” Our progress remains “too slow” online. We need to think faster, smarter, and take full advantage of basic security practices that would protect from many day-to-day threats. More broadly, Carlin emphasizes that little will change unless the fundamental designs and standards of the Internet—elements that are inherently insecure and have been since the beginning—are sufficiently updated with a focus on security by design.

## CONCLUSION

Carlin successfully highlights the development of cyber threats since the rise of the Internet and provides valuable, thought-provoking insight into cybersecurity. He presents useful questions and suggestions to prepare for the road ahead. In his conclusion Carlin is perhaps overly kind in his assessment of American values as they pertain to the cyber realm—China is not the only modern society making “Orwellian advancements” in facial recognition technology and “ubiquitous” video surveillance. Nevertheless, *Dawn of the Code War* is a sweeping yet intimate picture of the current cyber threat landscape that correctly emphasizes the priority of cyber defense. 🍷

**BOOK REVIEW**

Title: *Dawn of the Code War:*

*America's Battle Against Russia, China, and the Rising Global Cyber Threat*

Author: John P. Carlin with Garrett M. Graff

Publisher: Public Affairs (October 2018)

Hardback: 468 pages

Language: English

ISBN: 978-1-5417-7383-7

Price: \$30.00

# THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

 [cyberdefensereview.army.mil](http://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.