

# THE CYBER DEFENSE REVIEW

\*\*\*

Tactical Considerations for a Commander to Fight and Win  
in the Electromagnetic Spectrum

*Major General Patricia Frost*

*Captain Clifton McClung*

*Lieutenant Colonel Christopher Walls*

Preparing for Cyber Incidents with Physical Effects

*Chief Joseph W. Pfeifer*

An Airman's View of Deterrence and Cyberspace

*General Jay Raymond*



Smart Bases, Smart Decisions

*Dr. Harold J. Arata III*

*Mr. Brian L. Hale*

There IS No Cyber Defense

*Mr. Bryson Bort*

Strategic Blind-Spots on Cyber  
Threats, Vectors, and Campaigns

*Dr. Cathy Downes*

Countering the Cyber Threat

*Mr. Shawn Henry*

*Dr. Aaron F. Brantly*

The Role of Commercial End-to-End  
Secure Mobile Voice in Cyberspace

*Mr. Elad Yoran*

*Dr. Edward Amoroso*

# THE CYBER DEFENSE REVIEW



# THE CYBER DEFENSE REVIEW

## A DYNAMIC MULTIDISCIPLINARY DIALOGUE

### EDITOR IN CHIEF

Dr. Corvin J. Connolly

### MANAGING EDITOR

Dr. Jan Kallberg

### AREA EDITORS

Dr. Harold J. Arata III  
(Cybersecurity Strategy)

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

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

Dr. Chris Bronk  
(National Security)

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)

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

Dr. Fernando Maymi  
(Cyber Curricula/Autonomous Platforms)

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

Ms. Elizabeth Oren  
(Cultural Studies)

Dr. David Raymond  
(Network Security)

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

Dr. David Thomson  
(Cryptographic Processes/Information Theory)

Dr. Robert Thomson  
(Learning Algorithms/Computational Modeling)

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

### EDITORIAL BOARD

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

Dr. Amy Apon  
Clemson University

Dr. Chris Arney  
U.S. Military Academy

Dr. David Brumley  
Carnegie Mellon University

Dr. Martin Libicki  
U.S. Naval Academy

Ms. Merle Maigre  
NATO Cooperative Cyber Defence  
Centre of Excellence

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

Dr. Milton Mueller  
Georgia Tech School of Public Policy

Dr. Hy S. Rothstein  
Naval Postgraduate School

Dr. Bhavani Thuraisingham  
The University of Texas at Dallas

Prof. Tim Watson  
University of Warwick,  
United Kingdom

### CREATIVE DIRECTORS

Michelle Grierson  
Gina Daschbach

### LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

### PUBLIC AFFAIRS OFFICER

Lt. Col. Terence M. Kelley

### KEY CONTRIBUTORS

Clare Blackmon  
Nataliya Brantly  
Kate Brown  
Donald L. Carmel, Jr.

Erik Dean  
Sarah Gardner-Cox  
Kristin Kohler  
Eric Luke

Asuman Mielke  
Alfred Pacenza  
Irina Garrido de Stanton  
Melita Webb

### CONTACT

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

### SUBMISSIONS

*The Cyber Defense Review* welcomes  
submissions. Please contact us at  
[cyberdefensereview@usma.edu](mailto:cyberdefensereview@usma.edu).

### SUBSCRIBE

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

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

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

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

∞ Printed on Acid Free paper.

INTRODUCTION

FROM THE EDITOR	09	<i>The Cyber Defense Review: Building an Intellectual Framework</i>
-----------------	----	---

SENIOR LEADER PERSPECTIVE

MAJOR GENERAL PATRICIA FROST CAPTAIN CLIFTON MCCLUNG LIEUTENANT COLONEL CHRISTOPHER WALLS	15	Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum
CHIEF JOSEPH W. PFEIFER	27	Preparing for Cyber Incidents with Physical Effects
GENERAL JAY RAYMOND	35	An Airman’s View of Deterrence and Cyberspace

PROFESSIONAL COMMENTARY

BRYSON BORT	41	There IS No Cyber Defense
SHAWN HENRY DR. AARON F. BRANTLY	47	Countering the Cyber Threat
ELAD YORAN DR. EDWARD AMOROSO	56	The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace

RESEARCH ARTICLES

DR. HAROLD J. ARATA III BRIAN L. HALE	68	Smart Bases, Smart Decisions
DR. CATHY DOWNES	78	Strategic Blind-Spots on Cyber Threats, Vectors, and Campaigns
ELSA KANIA JOHN COSTELLO	104	The Strategic Support Force and the Future of Chinese Information Operations
NADIYA KOSTYUK SCOTT POWELL MATT SKACH	122	Determinants of the Cyber Escalation Ladder



# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆





## *The Cyber Defense Review:* Building an Intellectual Framework



### FROM THE EDITOR

**T**he *Cyber Defense Review* (CDR) is a scholarly journal published by the Army Cyber Institute at West Point. The CDR publishes original, unpublished, relevant and engaging content from across the cyber community and is the only unclassified Department of Defense sponsored journal that exclusively covers the cyber domain. The CDR engineers a multidisciplinary dialogue through thought-provoking research articles and essays on the strategic, operational, and tactical aspects of the cyber domain.

The CDR celebrates the establishment of its inaugural Editorial Board. This exceptional group of cyber leaders and scholars will give direction, discuss how to improve quality and reach, and serve as a channel for qualified input to increase CDR standing and product. It will ensure the overall success of the CDR in becoming the journal of choice for cyber practitioners. The Editorial Board will vote on different propositions, identify topics for themed and special issues, suggest new Board members, and provide influence, support, input, and act as CDR Ambassadors.

We are excited to report that JSTOR—the world's most prestigious digital library—will launch the CDR in April as part of their Security Studies collection. Through JSTOR, the CDR will reach 8,000 institutions and libraries in 160 countries. The online CDR continues to post thoroughly researched articles and blogs designed to stir rapid discussion within the broader cyber community. To read the most recent articles and blogs, visit <http://cyberdefensereview.army.mil/>.

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

The CDR wishes to thank the authors of the spring edition for their absorbing research articles and commentaries that have advanced the body of knowledge. The team extends its appreciation to MSG Jeff Morris, MAJ Charlie Lewis, Courtney Gordon-Tennant, and LTC Terry Kelley for their exceptional editing support. We also recognize Gina Daschbach and Michelle Grierson for their remarkable design and layout of the CDR.

As we continue to build upon the intellectual framework created by this journal, we encourage you to join the conversation! 

*The CDR Team*





# THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆



# Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum

---

Major General Patricia Frost

Captain Clifton McClung

Lieutenant Colonel Christopher Walls

Edited by: Lieutenant Colonel Daniel Huynh

## ABSTRACT

While the United States (US) fought two wars over the past decade, its adversaries were evolving their technology for fighting in the electromagnetic spectrum (EMS). In his 2014 monograph, Dr. Larry M. Wortzel writes “the PLA [Chinese People’s Liberation Army] is updating 21st century mechanized and joint operations, combining them with electronic warfare—what the PLA calls “fire power warfare”—and precision strike.”<sup>[1]</sup> New doctrinal concepts ranging from the tactical to operational levels of employing traditional signals intelligence and electronic warfare lead this change movement in China.<sup>[2]</sup> Included in the transition is cyber warfare, which details both kinetic and non-kinetic effects across the EMS.<sup>[3]</sup> We have seen similar advances in capability from Russia in the ongoing conflict in Ukraine. The Ukrainian military has witnessed first-hand the actual effectiveness of Russian electronic warfare (EW) technology and tactics.<sup>[4]</sup> Russian artillery has demonstrated the synergistic effects of EW and commercial off-the-shelf (COTS) small-UAS platforms when paired with jamming, indirect fire, and direct fire assets [in Ukraine].<sup>[5]</sup> The Russians have utilized EW capabilities to geolocate Ukrainian signals and their associated forces, then fixed the formation with UAS, and finished these forces with jamming of mission command frequencies while delivering devastating barrages.

While the U.S. Army modernized its network and networked systems, it also encountered a paradigm shift as the network transitioned from a service to a warfighting platform that is now critical to all Army operations. These advantages through the EMS have significantly increased each formation’s lethality from the infantry fire team to the brigade combat team. As a result, the Army significantly increased its reliance on devices and systems that communicate within the complex EMS to maintain this

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





Major General Patricia A. Frost assumed the role as Director of Cyber, Office of the Deputy Chief of Staff, G-3/5/7, Headquarters, Department of the Army in July 2016. A career intelligence officer, MG Frost has been working in the Cyber domain for the last 4 years.

MG Frost has held command and staff positions across all levels of the Army with assignments in the United States, Iraq, Afghanistan, Philippines, and Germany. Prior to her appointment as Director of Cyber, MG Frost served as the Deputy Commanding General for Operations for U.S. Army Cyber Command.

advantage. In Iraq and Afghanistan, the Army enjoyed overmatch in the spectrum without heavy investment in the modernization of EW capabilities due to the threat's inability to contest US capabilities in the EMS. Our adversaries in Iraq and Afghanistan relied mainly on commercial communications technologies. Meanwhile, other near-peer countries such as Russia and China made significant investments in modernizing and honing their EW skills and capabilities, which puts the US military at a significant disadvantage.

Army leaders have realized after shifting from the War on Terror to Multi-Domain Battle that there is a significant EW capability gap. With this realization that the US no longer enjoys an advantage in the EMS, the Army as a whole must adapt to the implications of operations in a complex EMS environment. The development of secure communication and other EMS capabilities must continue to be a priority for Army R&D and science and technology communities. The Army must also speed the process to bridge gaps through rapid capability development and agile acquisition processes. US adversaries already possess EW capabilities that provide overmatch, and the threat will continue to evolve. The Army must invest to transform as well to address this threat.

Historically our Soldiers were taught radio discipline; tactics such as only talking on a radio for three to five seconds, and the use of pro-words or brevity terms.<sup>[6]</sup> The rationale behind such brevity was that an enemy could triangulate using ES direction-finding (DF) capabilities to locate and target our position. Once located, the adversary could then engage with either jamming, direct, or indirect fire. Fast forward to the present day, and it is easy to see the impact of how technology has shaped the battlefield. SIGINT, EW, and DF technology has grown



Captain Clifton McClung is the Electronic Warfare Officer (EWO) for the Army Cyber Institute's (ACI) CEMA Integration Group (CIG). He commissioned as an Infantry Officer in 2008 and served as a Mechanized Infantry Platoon Leader and Battalion Signal Officer in the 3rd Infantry Division in support of Operation Iraqi Freedom and Operation New Dawn. From 2013-2016 he served as a Brigade EWO, Deception Planner, and S3 Plans Chief for three years in 1-2 Stryker Brigade Combat Team, Joint Base Lewis-McChord. As a member of ACI's CIG, he contributes to shaping the Army's Electronic Warfare strategy and the integration of emerging threat scenarios into combat training centers at the tactical level. CPT McClung is currently preparing to transition to graduate school to pursue a Master's Degree in Information Security and Technology.

exponentially faster and is more accurate and effective. Current COTS direction finding systems and EW equipment can rapidly triangulate the location of a transmitter. This provides a greater reason why the Army must leverage its experience and reinstitute our 'historical' training to reduce our signature when facing an adversary with advanced EW capabilities. We must make greater strides in integrating EW into combined arms maneuver, and more importantly, the Army must philosophically change the way it employs and exercises mission command throughout the Multi-Domain Battle Refocusing on EW and long-range precision fires capabilities will significantly enhance Army readiness for future conflicts.

Through a series of critical questions, this paper hopes to inspire the thought leadership required to operate in a complex EMS environment. It will further detail and discuss how and why mission command is so critical to the evolution of EW, and how we must change to fight and win in the EMS by increasing lethality. The current mode of Army EW operations will not achieve even a limited window of tactical advantage. Our Army's continued heavy reliance on devices and digital systems operating within the EMS will be our downfall if we do not recognize and work to mitigate our vulnerabilities, and our techniques for operating in a contested environment.

Commanders and their respective staffs face significant issues in the spectrum and should address certain questions to understand how to fight and win within the EMS.

- 1. How should I think differently about the operations process when it comes to an EMS environment that is highly congested, contested, and degraded?**  
Commanders must integrate integrate



Lieutenant Colonel Christopher Walls is a Cyber Warfare Officer, currently serving as the Deputy Division Chief for Strategy and Policy in the Cyber Directorate of the Department of the Army G3/5/7. He was commissioned as an Infantry Officer and served in both mechanized and airborne units with numerous combat deployments. In 2010, LTC Walls began his cyber career at U.S. Cyber Command and has since served operational and institutional assignments at Army Cyber Command and the Army Cyber Center of Excellence. Among LTC Walls many distinguished accomplishments, he most recently led the development of *Army Field Manual 3-12 Cyberspace and Electronic Warfare Operations* and is an acknowledged expert on full spectrum cyberspace operations within the Department of Defense.

SIGINT and EW operations into all phases of operations. As described in the recently published Army FM 3-12, the Cyber Electromagnetic Activities (CEMA) staff section is responsible to plan, integrate, and synchronize both offensive and defensive cyberspace and electronic warfare operations. The CEMA section utilizes existing processes, intelligence, collection management, military decision-making process (MDMP), targeting, and others to plan, integrate, and synchronize electronic warfare operations into a unit's operations. Commanders and staffs must integrate EW considerations into the planning and execution of operations to increase lethality and effectiveness. Specific examples include ensuring that commander's intent includes a vision for EW, requiring an electronic order of battle to understand threat EW capabilities, ensuring that intelligence requirements (IRs) are established, developing targeting guidance that addresses adversary EW capabilities, requiring and enforcing electronic protection measures, and integrating EW considerations into home-station training.

2. **How do I maintain situational awareness of my EMS signature?** Commanders and staffs must understand that the EMS signature is the electromagnetic radiation emitted by their unit's emitters, such as communication systems, and networked capabilities. These systems, based on the amount of power they are using, can produce a signature that adversary receivers can detect, locate, collect, and target with lethal and non-lethal effects. We need to evaluate the



Lieutenant Colonel Daniel P. Huynh serves as a senior cyber research scientist at the Army Cyber Institute. He is currently a Cyber Warfare officer, and a former Field Artillery officer and FA53, Information Systems Engineer. He is a 1999 graduate of the United States Military Academy with a Bachelor's Degree in Computer Science. Additionally, he has a Master's Degree in Computer Science from the Naval Post Graduate School. LTC Huynh's most recent assignment was with the Cyber National Mission Force, as a National Cyber Protection Team Operations Officer and Cyber Network Defense Manager. LTC Huynh holds numerous professional security certifications which include: CISSP, GXP, GPEN, GCFA, GMOB, MCITP, CASP, CEH, CSA, and SEC+.

use of these systems from a force protection and survivability perspective. We cannot afford to have continuous transmissions of hour-long Battlefield Update Briefs (BUBs) that occur throughout the day. Electronic protection measures provided by the CEMA section should include guidance on active and passive measures that unit and subordinate commanders can take to reduce their signature and increase survivability. All devices that transmit and provide a targetable signature must be carefully used to minimize risk. Commanders must assume risk only when operationally necessary. The risk of physical travel to meet to exchange information may be high, but still lower than creating a targetable signature for the adversary. Because of this threat, commanders should increase the use of mission-based orders enabling staff to understand and execute their intent and lower the requirement to continually transmit orders. Dissemination of products via the spectrum should also factor in the threat of enemy detection. Commanders should continue to stress and train disciplined initiative into their subordinates for them to execute operations based upon intent and reduced feedback loops.

3. **What types of EW assets are available to me? Which are organic and which must I request?** Capabilities available to commanders will vary by echelon and unit. Electronic warfare support (ES), actions taken to search identify and locate signals (and associated units) to support operations, can be conducted by organic EW or signals intelligence (SIGINT) systems. Actions taken

to conduct SIGINT and ES may be very similar and should be mutually supporting. Both capabilities can be used to answer intelligence requirements or support future operations. Ground, airborne, and terrestrial SIGINT platforms can confirm commander's critical information requirements (CCIR) to support the intelligence section and CEMA Cells' information requirements. CEMA and intelligence support can request joint platforms from the Navy, Marines, and Air Force.

There are a limited number of EW systems currently fielded, but additional capability is entering the force through Army rapid capability development and expedited acquisition efforts. While current systems are limited to short range dismounted and repurposed remote counter IED systems, future EW capabilities will include integrated dismounted, mounted, and aerial systems. Today's most relied upon system—the Prophet—can sense and identify emitters. When this system is integrated with other platforms, it can locate enemy emitters and multiple UAS systems. These systems are an improvement in capability for US forces, but are not suited for fighting a near-peer adversary with similar EW capabilities.

- 4. How can both ground and aerial EW assets enhance my Information Collection Plan?** The EMS environment may either be a target rich space or sparse landscape based upon adversarial tactics, techniques, and procedures. It is the staff's responsibility to help develop intelligence requirements and prioritize collection assets. The number of assets used against an adversary will always be a constraint, so it is critical to understand how both SIGINT and EW passive and active measures can affect each other. The Electronic Attack effect of communications denial (an example of an active measure) requires a detailed understanding of the adversary's communications architecture and allocation of additional EA resources to achieve a 'denial' effect. However, selective disruption, which may include periods of denial of specific systems, can be used to 'herd' the enemy from one system to another. The enemy is forced to exercise his PACE (Primary, Alternate, Contingency, and Emergency) plan, which can enhance SIGINT collection. As part of the greater collection and targeting plan, SIGINT collection and EW activities should be synchronized and de-conflicted to increase effectiveness and reduce unintended consequences.
- 5. What is the emission control (EMCON) posture by phase, and what are our triggers to shift in the PACE communications plan?** The S6, S2, and CEMA Cell must collaborate to identify where the enemy will locate collection and EW assets throughout the battlespace, and how they will likely be employed. Based on these assumptions, the S6 should develop a dynamic signal concept of utilizing friendly-based, enemy-based, terrain-based, and time-based triggers to shift the communications plan as required. This includes identifying windows ranging



from the limited use of continuous transmission of satellite communications to not deploying these systems at all. When the mission requires a higher discipline of EMCON to achieve surprise or survivability, the staff must also develop alternate communications to synchronize and maintain Mission Command at a minimum one-level up and one-level down. Examples include, but not limited to tactical radios using short data burst communications, convoy flag or hand and arm signals, and pyrotechnical signals.

- 6. How can I detect if my unit is experiencing an electronic attack?** Units should have battle drills in place to determine cause or sources of electromagnetic interference (EMI) to include troubleshooting of systems and determining breadth (frequency bandwidth and physical distance) of interference. One of the keys to successfully identifying the source of electromagnetic interference is accurate reporting in conjunction with analysis, while other collection capabilities can assist in determining the source of the EMI. Units must establish and implement EMI resolution procedures as described in Enclosure D “EMI Characterization and Resolution at the Local Level”; CJCSM 3320.02A, “Joint Spectrum Interference Resolution (JSIR) Procedures”, for every mission command system.<sup>[7]</sup> These procedures are a Soldier skill, and just as important as learning how to load, clear, and reduce stoppage on an assigned weapon system. Since it is entirely possible that the Soldier will come in contact with EW effects prior to direct fire contact with similar or greater consequences it is imperative to train our forces to recognize and respond to indicators of an electronic attack. The CEMA Section at echelon may tailor the joint doctrinal procedures, and create their own battle drills and standard operating procedures for their specific echelon and mission.

*Some basic questions, tied to CCIR, to ask during interference would be:*

- ◆ What specific radios or systems affected?
- ◆ Are alternate frequencies affected?
- ◆ Who and where are the affected units?
- ◆ Is disruption occurring laterally and vertically across the unit?
- ◆ Can friendly systems’ frequency, Julian date, time, or hopset be changed?
- ◆ Can friendly forces use a system in another band or frequency?
- ◆ Have you submitted SIGINT requests for collection for your frequencies, in front of the forward line of troops (FLOT), at a higher power level than yours to identify possible enemy EA effects; and if so, are you now cross-cuing with imagery intelligence (IMINT) to confirm enemy systems in that area?

- ◆ While the S6 may focus on the standard troubleshooting of internal and external communication, they should also share information with the S2 and CEMA cell to process proper reporting to higher headquarters. This request could be made through a Joint Spectrum Interference Report (JSIR) by the unit(s) experiencing EMI and submitted vertically to the respective CEMA Section/S6/G6 (ref. Enclosure E “Joint Spectrum Interference Report format”; CJCSM 3320.02A, “Joint Spectrum Interference Resolution (JSIR) Procedures”).<sup>[8]</sup> It is highly recommended that unit S6/G6s build and disseminate a JSIR format for radio and digital systems for increased efficiency and accuracy of reporting; e.g., making and publishing a fill-in-the-blank JSIR for JCR similar to a call for fire request. Typically only SIGINT platforms at brigade and above can confirm or deny if interference is the result of adversary EW effects. It is immaterial to the type of interference (technical communications issue or enemy overt/covert EA effects) at company or battalion levels; units should shift in their PACE plan and continue the mission.

**7. How can we minimize and mask our EM signature from the enemy?** The use of terrain to mask transmissions from combat network radio (CNR) propagating toward enemy collection platforms should be implemented whenever possible as a tradeoff to extending CNR range. For example, the masking of electronic signatures by establishing radio transmission sites on the military crest of hilltop versus the physical crest to mitigate radio wave propagation into enemy EW or SIGINT systems. The same terrain that will impede your ability to communicate from surface to surface communications, such as large stands of trees or dense vegetation, hills obstructing line of sight, and potentially large bodies of standing water, will affect the enemy’s ability to use their organic ground-based ES assets to collect signals of interest. If the enemy is using an airborne EW or SIGINT platform, even high frequency (HF) radio communications have an increased risk of direction finding or jamming. The use of masking communications emissions with terrain can decrease the probability of detection and jamming. Radio frequency line of sight is often much greater than physical line of sight. Some radio signals and energy can “bend”, reflect, or refract off or around terrain, thus both extending your ability to communicate and the enemy’s ability to direction find or jam. If the enemy attempts to jam a CNR network that you are retransmitting around your area of operations, you could potentially retransmit the enemy’s jamming signal as well, thus another reason to mask your CNR retransmission sites. This will reduce your CNR footprint, but increase survivability and preserve mission command.

Minimizing EM signatures ties into and reinforces the previous point about the use of out of band methods to communicate. The enemy cannot detect and locate a unit that does not transit nor identify a unit that is continuously obfuscating themselves and implementing an effective electronic protection plan by shifting in their communications frequency bands.

8. **How can I assess my unit's digital and electromagnetic spectrum footprint during training and while deployed?** As described in the new FM 3-12, the Spectrum Manager, who works for the cyber planner in the CEMA Cell, is responsible for maintaining the situational understanding of the EM environment. This is accomplished through the deployment of organic directional and omnidirectional spectrum analysis equipment. This same equipment could be used to locate sources of interference but requires a deliberate sustainment training plan to maintain a highly technical and perishable skillset. A spectrum manager will have a significantly harder time identifying the source of interference if they do not have the equipment or training to establish an EMS baseline in their operating area to compare before and after experiencing interference. These requirements are new to spectrum managers and will require commander support to enable these individuals to grow into this new mission.
9. **How do we train to fight and win in a degraded or contested EMS during Home Station Training (HST)?** We emphasize CEMA at HST because you should not rely on your next Combat Training Center rotation to train in a contested or degraded EMS environment. Integrating EW individual, collective, or staff battle drill tasks into all major training exercises is a key component to maintaining Mission Command and physical survivability. HST should be done at all levels and include a mix of live play use of available systems, constructive effects, and/or conceptual TOC or communication exercises. Generic adversary EW capabilities is a good starting point for how CEMA effects should be integrated into HST. Whether the replicated threat is notional or simulated, units still need to have the necessary confidence and basic proficiency in their digital and communication systems. Their ability to recognize and respond to adversary EW activities should be achieved through routine digital gunnery. Only through repeated practice and rehearsals of decentralized mission command, execution of communication PACE plans, and deliberate out of band communication will units improve their readiness levels. Units must also integrate CEMA into planning and operational processes. Whether your unit is utilizing internal assets or requesting external assets (live or constructive), creativity and experimentation can go far in ensuring training is realistic and challenging. The repurposing of a Combat Network Retransmission (CNR) team to attack a portion of an operational radio network is an example of how a unit might replicate enemy EW effects. Localized GPS jammers might also be



used to reinforce analog battle tracking, navigation, and fire mission processing. While conducting training, it is essential to recognize the need for advanced coordination with your Range Control and Local Spectrum Management office. Lead times for approval for use due to the required coordination may take weeks to months for initial requests, so allow extra time to ensure proper coordination.

- 10. How can my staff and I further increase our knowledge and understanding of CEMA planning considerations?** A great starting point for references is FM 3-12 Cyberspace and Electronic Warfare Operations dated April 2017. Additional recommended professional reading is from the valuable repository of Lessons Learned from CTC “CEMA Support to Corps and Below” rotations supported by U.S. Army Cyber Command (ARCYBER). The RAND Corporation recently published two worthy studies on Tactical Cyber employment for Corps and Below.<sup>[9]</sup> Regarding training, a relevant course for staff would be Army Leader Cyber Operations Course (ALCOC), which gives the fundamentals of Cyber and EW employment considerations. A course that non-EW personnel may take for familiarization with Army and Joint EW concepts, fundamentals, doctrine, and capabilities is the Electronic Warfare Integration Course (EWIC). This course is 40-hours and is taught by 1st Information Operations (IO) Command to provide IO Officers familiarization for incorporating EW support to Information Operations. The 1st IO Command offers two other courses that EW personnel at brigade and above could attend: Military Deception Planners’ Course and Cyberspace Operations Integration Course.<sup>[10]</sup> For additional reference material for EW Officers and Warrant Officers, see DA PAM 600-3.<sup>[11]</sup> Lastly, it would be wise to lean heavily on your BCT’s EWO and EWO Technicians to be the subject matter experts in this area, and to provide Leader Professional Development (LPD) training for you and the staff.

## **CONCLUSION**

As a commander, fighting and winning within the EMS does not require a degree in Electronic Warfare. However, being a commander who embraces the need for an evolution in thought about mission command will undoubtedly improve unit readiness and set the right conditions to win on the battlefield of today and tomorrow. The importance of fostering an environment that emphasizes disciplined initiative is not a new idea, but when put into context against a realistic threat who can directly affect mission command through EW means, only further drives home this topic of relevance. As with many other competing priorities that a commander and staff must deal with, CEMA is not something that can be dealt with as an after-thought. The integration of CEMA into all warfighting functions will increase our Joint warfighting capability. Only by placing emphasis and resources towards training CEMA, will staffs and subordinate units improve their understanding

and proficiency. Even though the Army still has many roads ahead to conquer with the integration of both friendly and enemy EW capabilities into live, virtual, and constructive training—this should not preclude tactical units from experimenting with and getting creative in training CEMA now. Understanding where we are in today’s military environment, and where we are going with technology, one might think about a continuum of how we should train. Whether we are fully automated and digital, or fully analog and manual, we must not lose sight of how important and influential a commander’s personal emphasis, training guidance, and philosophy can be in shaping the EMS fight. 🛡️

## NOTES

1. China have spent their military budgets on modernization of EW doctrine, <http://www.dtic.mil/dtic/tr/fulltext/u2/a596797.pdf>.
2. “Russia have spent their military budgets on modernization of EW”, <http://thediplomat.com/2016/04/russias-surging-electronic-warfare-capabilities/>.
3. Russia destroys 85% of two Ukrainian Army Battalion, <http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/>.
4. <https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/>.
5. <http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/>.
6. STP 21-2 (Warrior Skill Level 1); CH 3, Task: 113-COM-1022, “perform voice communications”.
7. Enclosure D “EMI Characterization and Resolution at the Local Level”; CJCSM 3320.02A, “Joint Spectrum Interference Resolution (JSIR) Procedures, January 20, 2006.
8. Enclosure E “Joint Spectrum Interference Report format”; CJCSM 3320.02A, “Joint Spectrum Interference Resolution (JSIR) Procedures, January 20, 2006.
9. RAND Corporation, “Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below”, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1600/RR1600/RAND\\_RR1600.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf); RAND Corporation, “Reimagining the Character of Urban Operations for the U.S. Army: How the Past Can Inform the Present and Future”, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1600/RR1602/RAND\\_RR1602.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1602/RAND_RR1602.pdf).
10. 1st Information Operations Command sponsored courses, <http://www.lstiocmd.army.mil/Home/iotraining>.
11. U.S. Army, DA PAM 600-3 “Commissioned Officer Professional Development and Career Management”, 26 June, 2017.

# Preparing for Cyber Incidents with Physical Effects

---

Joseph W. Pfeifer

## ABSTRACT

Cyber weapons have been used to steal billions of dollars of intellectual property, influence elections, manipulate news and damage critical infrastructure. Yet, we think of cyberattacks as only a technology problem, which are handled by smart computer network technicians capable of discovering a breach and developing patches to mitigate the problem. Certainly, technical solutions are a big part of cyber preparedness. But what if cyberattacks combine denial of services in cyberspace with targeted attacks on critical infrastructure, causing massive damage and loss of life in the physical world?

This article will explore how federal, state, and local agencies, as well as private corporations, are using tabletop exercises, functional simulations and war gaming to prepare for significant cyberattacks. These programs examine how public and private sectors adapt to extreme cyber events. In a connected world, adaptive incident managers quickly form networks to exchange ideas, align core efforts and foster public communication.

### *Designing Cyber Exercise*

Today's threat environment of state-actors, terrorists, criminals, and hackers could use cyberattacks to cause physical harm as a substitute for kinetic assaults. This dramatic shift from guns and bombs changes how we perceive risk and preparedness. Cyber exercises need to identify gaps in prevention, protection, mitigation, response and recovery procedures. However, well-designed exercises also create the conditions to develop new skills and partnerships for managing the impact of a cyber event. Examining the experience of exercise participants is not only about observing behavior, but also is about understanding cognitive processes when overwhelmed by mass destruction that has not been fully imagined. Exercises, simulations and war games

©2017 Joseph W. Pfeifer



Joseph Pfeifer is the Chief of Counterterrorism and Emergency Preparedness for the New York City Fire Department (FDNY). During his career, he has commanded responses to some of the largest disasters in New York City's history. He was the first Chief at the World Trade Center attack on September 11, 2001, played a major command role during Hurricane Sandy in 2012, and helped manage NYC's Ebola Response. He is the founding director of FDNY's Center for Terrorism and Disaster Preparedness, a senior fellow at the Combating Terrorism Center at West Point, and a senior fellow at the Program on Crisis Leadership at the Harvard Kennedy School. Pfeifer has spoken at United Nations Conferences and the World Knowledge Forum, and testified to the U.S. Congress about the threats cities will face in future. He holds Master's Degrees from the Harvard Kennedy School, Naval Postgraduate School, and Immaculate Conception and has written widely in professional journals.

are ways to gain insight into decision-making when under stress and confronted with novelty.

Over the past year, three noteworthy cyber exercises were conducted to build a framework for mitigation and response to multi-sector cyberattacks on major cities. The first was by the Army Cyber Institute (ACI) in cooperation with New York City agencies (FDNY, NYPD, NYCEM, DOITT, DEP) and Citigroup. The ACI designed an exercise that combined a functional computer keyboard operator piece requiring technicians to defend the network against a "live-fire" from an opposing "red team" in a virtual environment, along with a tabletop exercise for senior leaders from the emergency response community, water supply, utilities, banking, telecommunication, health, and transportation. This two-day exercise was useful because it promoted interactions between technicians and emergency response leaders.<sup>[1]</sup>

The second exercise was a simulation conducted by FDNY's *Center for Terrorism and Disaster Preparedness (CTDP)* for cadets from the United States Military Academy at West Point. Cadets enrolled in Homeland Security and Cyber classes were brought to the FDNY's Operation Center in Brooklyn to participate in a realistic simulation. These cadets formed an Incident Management Team (IMT) that managed state and local responders who worked with military assets during a cyber incident with physical effects on New York City. They then had to report their operational plan to FDNY's Chief Counterterrorism and The New York Adjutant General of the National Guard who were part of the exercise. Utilizing an IMT to handle the consequences of a cyberattack with physical damage proved invaluable to coordinating a multi-sector response.<sup>[2]</sup> The IMT shared information across sectors and coordinated federal, state and local operations.

The third exercise was a series of cyberwar games designed by Naval War College (NWC) against private sector critical infrastructure. With 85% of all critical infrastructure owned by the private sector, senior leaders from 15 critical infrastructure sectors, including financial services, food and agriculture, chemical, energy, dams, wastewater, defense industry, healthcare, and communication, committed two full days to war gaming.<sup>[3]</sup> These industries engaged with Department of Defense (DoD), federal, state and local officials in war games that simulated targeted attacks by nation and non-state actors on U.S. critical infrastructure. The task was to manage the cyber and physical events as senior leaders kept government officials, infrastructure owners and the public informed.<sup>[4]</sup>

While each of these exercises had a slightly different focus, they all shared a common scenario of a major cyberattack on critical infrastructure in a densely-populated city. Events included distributed-denial-of-services (DDoS) attacks on the financial sector, hospital medical information ransomware demands, and physical destruction by manipulating Program Logic Controllers (PLC) and Supervised Control and Data Acquisition (SCADA) systems. The effect of the cyberattacks released hazardous radiation and chemicals, contaminated water and food supplies, crippled parts of the electrical power grid and communication systems, denied 911 telephone services (TDoS), and triggered air, rail, and road transportation accidents.

The exercise designers arranged a series of cyberattacks to create cascading effects across sectors. As systems become more interdependent, cross-sector cyberattacks increase the risk of catastrophic consequences. This is especially concerning when there are few cross-sector ties for information-sharing and crisis management during cyber with physical damage.

### ***Sharing Information and Situational Awareness***

As the cyber exercises unfolded, operators of critical infrastructure and emergency responders were absorbed by events that appeared to look almost routine. The financial sector questioned why their ATMs were not working, as emergency responders were called to multiple emergencies. Each sector, influenced by organizational bias, became so preoccupied with solving their own problem that they became oblivious to what was occurring outside their group.<sup>[5]</sup> But with the spread of service outages and an uptick of emergencies, there was a need for greater situational awareness regarding the entire event.

Situational awareness is a threefold process of perception, comprehension, and anticipation.<sup>[6]</sup> During a significant cyberattack, this search for situational awareness becomes more complicated as senior leaders and organization fail to recognize the signs that events are taking place across both the cyber and physical domains. This is further obscured by not understanding the interdependency of these two worlds and the inability to anticipate what could happen next.

All three exercises illustrate the struggle to fully comprehend the connections between a cyberattack and the resulting physical events. Failure to acquire multiple levels of situational awareness limits one's ability to manage and mitigate the incident. Organizations turn into themselves and focus only on their presenting problems. Even when organizations wanted to grasp the bigger picture, there was a lack of knowing how to share information and who to collaborate with across sectors.

The *National Cyber Incident Response Plan*, based on *Presidential Preparedness Directive 41*, attempts to address this gap in information sharing and coordination.<sup>[7]</sup> It calls for the private sector to report cyber incidents to their Information Sharing Analysis Center (ISAC), arranged by particular sectors, e.g., financial, chemical, energy, etc. The plan also talks about the FBI sharing information with the intelligence community. Influenced by organizational bias, these well-intended procedures can create *stovepipe situational awareness*, where information is only shared within a particular sector.

Connecting diverse groups of people during a cyber-attack to share information at the physical incident and away from the incident in a computer center is the challenge. In most exercises, participants make these connections notionally. However, the ability to connect through voice, video, and data is critical for information sharing. Cyber exercises have identified the lack of knowing how and who to connect at the federal, state and local levels as a significant gap in preparedness. Organizations and sectors need to be able to push and pull information not only about their part of the incident, but also about the global effects of the incident.

As part of an improvement plan, we must explore how to map out network ties for information sharing during cyber events. Constructing a network map would visually display what agencies need to connect to each other for situational awareness. This could be tasked to Department of Homeland Security (DHS) Fusion Centers, whose main function is to share information for homeland security. These state and urban area Fusion Centers do not command or control resources; instead, they should become the conduit for moving information so others in government and the private sector can better exchange ideas and align core efforts. Fusion Centers form information hubs, which decentralize the flow for more timely and accurate reporting.

### ***Managing the Incident***

The next preparedness advancement in cybersecurity is to develop the skills to manage an incident in the dual world of cyber with physical effects. While malware can be planted in systems long before an attack takes place, a significant cyberattack with physical effects will most likely take place quickly to shock and avoid adaptive response. The initial shock and cumulative stress of an evolving incident could cause a loss of system control, stovepipe situational awareness, ineffective coordination, and a drop in public confidence for government to mitigate the damage.

As a cyber incident begins, technicians start to connect to each other to mitigate the attack on their systems. If these attacks have physical effects, first responders will form teams of firefighters, police officers, and EMTs/paramedics to jointly respond to the emergencies. At the same time, federal, state and the local Emergency Operations Center and the National Cybersecurity and Communications Integration Center will start to connect to each other to build a comprehensive operating and resource assessment picture. The National Guard and federal resources will also begin to mobilize assets to mitigate the incident. How these groups form vary greatly depending on if they emerge from the federal, state or local levels. Connecting these groups requires the creation of hastily constructed communication networks.<sup>[8]</sup>

A network structure emerges when parts of the public and private sectors begin to connect and coordinate with each other. The same evolutionary process occurs for crisis management during other catastrophic events such as natural disasters, terrorist attacks, large-scale accidents, and major wildland fires. At the early stages of an incident, random networks appear, then emerge into a more organized cluster pattern, and finally when an incident is nearly stabilized a more centralized hub-type network begins to form. Response to extreme cyber events is a process of emergence that starts with a convergence of public and private sector response groups that self-organize into a more connected network. From little order emerges a complex social system of clusters. Each central node shares information within and outside its cluster, which begins to create a network system of incident management.

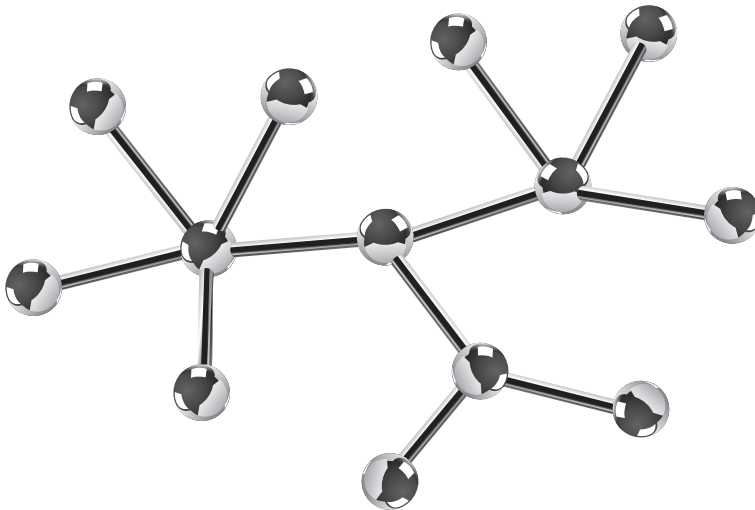


Figure 1. Networks connect public and private sectors for information sharing, response coordination and public messaging.



Crisis leadership is about forming clusters and getting clusters to communicate and coordinate with each other. The *National Response Plan* (NRP), *National Incident Management System* (NIMS) and *National Cyber Incident Response Plan* provide a framework for incident management. NIMS, in particular, can play a significant role in shaping the physical and cyber management space, yet this is rarely used in cyber exercises. The problem is that incident management is viewed as a hierarchical, top-down structure, when in reality incident management emerges from the bottom up. During a significant cyber incident, there are many different response organizations separated by geography and function. The incident management system guides the building of a management structure that includes elements of command, operations, planning, logistics, and administration. As the incident grows, clusters form area commands, which connect to other clusters (hubs) for information and resources. The actual shape of the response network is dependent on the ties between clusters.

IMT's trained for a cyber incident with physical effects can play an essential part in shaping the cyber incident response network. These teams are different than the Computer Emergency Response Team (CERT) whose function is to mitigate computer security incidents on the network side. A Cyber-IMT, similar to the West Point cadet simulation, bridges the gap between the cyber and physical world by connecting technical cyber mitigation with different parts of the response network for information sharing and incident management. Building these teams with the trained personnel will take a considerable amount of effort, which could be tasked to each FEMA region. Such efforts are beginning to be discussed by DHS and others in the private sector. In the energy sector, they are exploring the idea of "Cyber Consultants." These Cyber-IMTs could be incorporated nicely into the *National Cyber Incident Response Plans*.

### ***Communicating with the Public***

Since every significant cyber incident is political, the third component of cyber preparedness is the ability to communicate with the public and government officials. This involves public messaging, press briefings, countering fake news, and holding conference calls with officials from the federal, state, and local government. All three exercises tested public communications. One simulation used video cameras and microphones with tough reporters to simulate a real press briefing. The spokesperson must be knowledgeable about what is occurring, empathetic to the people affected by the incident, and explain what is being done to manage the incident. Complicating public messaging is fake news, which could be misinformation and part of the cyberattack or simply rumor. In any case, frequent updates to the public are useful countermeasures.

Public officials have a responsibility to effectively manage information and the incident. Therefore conference calls with Secretaries, Governors, Mayors, and other officials are extremely important. At times, it may be beneficial to include the CEO of critical

infrastructure as part of this call. These conference calls need to be held at least once a day. This political communication engagement is a critical element of cyber exercises that should be tested with at least senior leaders' staffers.

### ***Preparing for the Future***

Cyber preparedness leverages exercises, simulations, and war games to strengthen a response network for information sharing, incident management, and public communication. This network model of public and private sectors is flexible enough to adapt and respond to cyber incidents with physical effects. The challenge is to pinpoint the connections or ties that shape the network of cyber and emergency response partners. These connections bridge gaps between the cyber and physical world for exchanging critical information and coordinating response efforts. Even a small number of bridging ties can dramatically accelerate the spread of information within a system.<sup>[9]</sup> Senior leaders are dependent on timely information for situational awareness so they can make decisions that shape a response network to mitigate the effects of cyberattacks.

General (Ret.) Stanley McChrystal argues that robustness is achieved by strengthening parts of the system, while resilience is the results of linking elements that allow resources to be reconfigured or adapted to a changing environment.<sup>[10]</sup> He refers to this as *Team of Teams* working on different parts of a mission. In our attack scenario, it requires multiple teams to manage the incident in the virtual and physical world.

Cybersecurity is about strengthening prevention efforts and mitigating attacks in this domain. Cyber preparedness is not only about cybersecurity, but it is also about coordinating a response in the physical world. This will take teams of people from both the public and private sectors. The challenge to maintain homeland security and business continuity is to understand how to reconfigure the network of teams to leverage each other to manage both the cyber and physical dimensions of an attack. 🛡️

## NOTES

1. Army Cyber Institute, *After Action Review*, (West Point), 2016. This Cyber exercise, named Jack Voltaic, is the first in a series of ACI multi-sector cyber and dual function (mitigation/response) exercises with major cities.
2. FDNY, *After Action Review*, (New York), 2017.
3. J. Schneider, *Cyber Attacks on Critical Infrastructure*, Insight from War Gaming, <https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming>, 2017.
4. Naval War College, *War Gaming Exercise Plan*. (Newport, RI), 2017.
5. Joseph Pfeifer, “Crisis Leadership: The Art of Adapting to Extreme Events.” *Harvard Kennedy School’s Program on Crisis Leadership Discussion Paper Series*, (Cambridge, MA: Harvard Kennedy School: 2013), 5.
6. Mica Endsley, *Toward a theory of situation awareness in dynamic systems*, Human Factors [H.W. Wilson - AST], Mar 1995, Vol. 37, 32.
7. DHS, *National Cyber Incident Response Plan*, (Washington, D.C., 2016).
8. P.J. Denning, Hastily formed networks. *Communication of the ACM*, 49(4), 2006, 15-20.
9. David Lazer and Maria Christina Binz-Scharf, “It Takes a Network to Build a Network” in *Governance and Information Technology: From Electronic Government to Information Government*, edited by Viktor Mayer-Schonberger and David Lazer, (Cambridge: The MIT Pres, 2007), 266.
10. Stanley McChrystal with Tatum Collins, David Silverman, and Chris Fussel, *Team of Teams: New Rules of Engagement for a Complex World*, (New York: Portfolio/Penguin, 2015), 80.

# An Airman's View on Deterrence and Cyberspace

---

General Jay Raymond

*"Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our federal networks, and attack tools and devices that Americans use every day to communicate and conduct business."*

*- US National Security Strategy, Dec 2017*

*"Russian cyberattacks have targeted the White House, the Joint Staff, the State Department, and our critical infrastructure...Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the U.S. Navy, U.S. partners in the Middle East, major U.S. financial institutions, and a dam just 25 miles north of New York City. And of course, North Korea was responsible for the massive cyberattack on Sony Pictures in 2014. What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk."*

*- Senator John McCain, Jan 2017*

Deterrence, military strategy, and national power are taught at all our United States service academies. As a military officer, you will repeatedly study these subjects as you mature and grow into more senior positions. In this article, I would like to share with you my thoughts on deterrence, and what we have been doing to improve our ability in the Air Force to fly, fight and win-in, thru, and from cyberspace.

From the mid-to-late 80s, my duty was to stand watch in a Minuteman ICBM missile capsule near Grand Forks Air Force Base, North Dakota. Because of this experience,

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



Gen. John W. "Jay" Raymond is the Commander, Air Force Space Command (Air Forces Strategic-Space) and the Joint Force Space Component Commander, U.S. Strategic Command, Peterson Air Force Base, Colorado. General Raymond is responsible for organizing, training, equipping and maintaining mission-ready space, cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands. He directs USSTRATCOM space forces providing tailored, responsive, theater and global space effects in support of national objectives.

General Raymond was commissioned through the ROTC program at Clemson University in 1984. He has commanded at all levels of Air Force organization. His joint assignments include the Office of the Secretary of Defense, U.S. Strategic Command, Commander, Joint Functional Component Command for Space and currently Commander, Joint Force Space Component Command. Additionally, he served as the Director of Space Forces, as a Colonel, in support of operations Enduring Freedom and Iraqi Freedom at the USCENTCOM CAOC.

I learned early in my career that in the military, every task matters. With this contextual experience of the importance of readiness and lethality firmly engrained in my psyche, I left Grand Forks. One month later, the Berlin Wall fell, the Cold War began to melt, and our nation began to think through the implications of a non-bipolar world. Twenty-three years later, I found myself stationed at U.S. Strategic Command, challenged with a resurgent Russia, and an expanded set of potential adversaries. Deterrence remained a cornerstone of US security, but the range of actors and the complexity of challenges required a re-evaluation of deterrence approaches. Today, I find myself charged with Air Force responsibilities for organizing, training and equipping both space and cyberspace forces. And once again, the complexity and range of actors needed to be deterred have expanded. But as a military officer and a practitioner of national security, one thing has remained constant; peace is best preserved from a position of strength, and military strength is derived from readiness which fuels lethality.

Today's geopolitical environment demands a tailored, flexible, and clear strategy that is communicated, resourced and continuously executed. A good strategy articulates ends and explains the ways and means that instruments of national power are orchestrated to achieve those ends. Good strategy calculates risk and captures opportunities advantageous to our Nation for sustained success.

Deterrence is the cornerstone of our Nation's security strategy. Deterrence occurs in an adversary's decision calculus. It does not manifest itself in isolation within a particular domain of warfare. The decision to not act is a holistic summation of the larger circumstance and environment. Ultimately, if we desire to shape and deter an adversary's behavior in cyberspace, we must address deterrence

from an integrated domain perspective and coherently leverage all elements of our national power to achieve our ends.

A deterrence strategy crafted to deny an adversary the benefit of attack is a necessary first step. The second step is to credibly threaten the imposition of a retaliatory action (i.e., impose cost). Our deterrence strategy should also consider the adversary's perceptions of the cost and benefit of inaction where possible.

For the executive branch, the Department of Homeland Security serves as the lead agency for critical infrastructure and key resource defense. Most recently, in 2017, the federal government added electoral systems to the previous list of 16 critical infrastructure/key resources for protection. For the military, our cyberspace mission is more narrowly focused. We operate Department of Defense (DoD) information systems and networks, and protect and defend them against cyberspace attack. When directed, we further enable our military forces' ability to operate in, thru, and from cyberspace at the time and place of our choosing. This encompasses both defensive and offensive cyberspace operations.

Within the Air Force, we have been aggressively pursuing integrated-domain approaches to fortify our contribution to our Nation's deterrence posture. Well-known is our ability to globally find, fix, target and strike. Less known are the Air Force initiatives in cyberspace. To deny an adversary the benefit of an attack, we have hardened our cyberspace perimeter at the enterprise level, collapsed hundreds of networks into one defensible Air Force Network (AFNET), and built defensive maneuver forces to quickly allocate against emerging threats. At the base level, we are transforming our traditional communications squadrons into cyberspace operations squadrons charged with meeting their senior commander's need to assure and protect the organization's mission.

At most Air Force installations, the Cyberspace Squadron Initiative translates into readiness that rapidly generates air and space power when called upon in support of the Nation. Furthermore, across the Air Force, our Materiel Command has partnered and led the expansion of cybersecurity beyond the traditional desktop and laptop environment onto and into our actual weapons systems, such as aircraft, spacecraft, armaments and supporting network control infrastructure. Our adversaries fear the U.S. Air Force in the air and space; hence we suspect they will seek to ground us before and throughout the fight. Our dependence in the air domain has grown over time. The F-4 Phantom, flown by the Air Force from 1963 until 1996, had only 8 percent of its functions performed by software. In contrast, one of today's fifth-generation fighter aircraft, such as the F-22 Raptor, is 80% dependent on computer technology (Demir 2009). This rapid increase in software reliance on our military weapon systems fuels our warfighting advantage on the battlefield, but it has also increased the criticality of cyberspace assurance. From the factory to the flight line, the Air Force is working to ensure our ability to generate and deliver global vigilance, reach, and power in and through a contested cyberspace

domain. From a defensive perspective, Air Force bases and weapons systems represent critical cyberspace terrain that we are urgently shaping to meet this emergent need.

Today, our AFNET enables the command and control of our force and support operations. But today's AFNET and secure network encumber many of our cyberspace operators with network administration tasks and information technology (IT) provisioning functions. The next step in our transformational journey is to realign these forces and expand our cyberspace defensive maneuver capacity. To achieve this end, the Air Force is shaping its IT provisioning services and IT commodities toward fee-for-service contract models. This approach is designed to allow repositioning of our cyberspace-focused Airmen from provisioning IT and services to defending key cyberspace terrain to enable global Air Force operations. All of these efforts are essential to improve our defensive posture, deny the adversary the benefit of an attack, and ultimately to shape adversary perceptions.

As our National Security Strategy (NSS) states, "The U.S. will deter, defend, and when necessary defeat malicious actors who use cyberspace capabilities against the U.S. When faced with the opportunity to take action against malicious actors in cyberspace, the U.S. will be risk informed, but not risk averse, in considering our options." To support the credibility and lethality necessary for deterrence and to decisively respond if deterrence fails, 29 of 39 Air Force-provided Cyber Mission Force teams have reached full operational capability. All 39 Air Force teams are on track for FOC by June 30, 2018, three months ahead of U.S. Cyber Command's (USCYBERCOM) target date. These units, in combination with our sister service teams, will provide USCYBERCOM 133 cyber teams comprised of roughly 6,200 personnel.

Like the missile forces of yesterday and today, our cyberspace assets must train, stay vigilant, and be ready. Their readiness incentivizes adversary restraint by signaling our ability to deny benefit and impose cost thus enhancing deterrence. In August 2017, the President directed USCYBERCOM be elevated to a full combatant command. Active planning to meet this direction is currently underway within the DoD, as USCYBERCOM prepares for full-spectrum military cyberspace operations to ensure US and Allied freedom of action in cyberspace. This further signals US commitment to provide our freedom of action in, thru and from the domain to both Allies and potential adversaries.

The NSS makes clear our intent to protect critical infrastructure and deter and disrupt malicious cyber actors, but in the 21st century, no domain can be understood in isolation. Our ability to deter action in air, land, sea, space, and cyberspace is a manifestation of the collective strength we present across all domains. Conversely, a weakness in any domain undercuts our readiness, hamstringing our lethality and erodes our credibility to deter. America's Airmen represent critical threads in the fabric of our Nation's integrated deterrence strategy. Whether on a keyboard, in a cockpit, or deep in a silo, America's Air Force stands ready to deliver Global Vigilance, Global Reach and Global Power, in, thru and from air, space, and cyberspace. 🇺🇸

# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆





# There IS No Cyber Defense

---

Bryson Bort

## ABSTRACT

There is a general principle driving the massive cybersecurity ecosystem that has flourished from the beginning: the necessary trade-off in balancing ease of deployment, the simplicity of operation, stability, and efficacy. While the entire ecosystem is predicated on constraints inherent in the foundational architecture, most in the defender community do not realize or understand what these are.

Reliance on flawed fundamental assumptions from what worked years ago has led us to a deeply entrenched, but intrinsically vulnerable environment that is continually compromised by an endless number of exploits. Exploitation occurs in an infinite space that is unsolvable. We are building skyscrapers on quicksand, yet are surprised when they fall.

Well-intentioned defenders, faced with constant attacks, compensate for this situation in two primary ways. We enthusiastically buy new tools, of which there is an endless supply, promising not only new but better results. And we aggressively build overlapping defense-in-depth, seeking comfort from the expertly plotted proverbial Venn-diagram that illustrates the breadth of our robust defensive portfolios.

But what actually works? In 2017, a CISO confided to me that while breaches are terrible, no good, evil things, he looks forward to an intrusion. It's the only chance he gets at some level of real validation of his defense infrastructure—both what worked and what didn't.

In fairness, security product offerings typically start out being useful. Everyone is excited about the next great thing, but as it achieves enough critical mass, it registers on attackers' radar. Then the product's efficacy begins to diminish, leading at best to the disappointing but often seen product half-life.

©2017 Bryson Bort



Bryson Bort is the Founderr/CEO of SCYTHE, Founder/Chairman of GRIMM, and Founding Member of the ICS Village, a non-profit advancing education and awareness of security for industrial control systems. Prior, Bryson led an elite Computer Network Operations research & development (R&D) division that directly contributed towards national security. Because of his background as an Army Officer and extensive operational cybersecurity experience, Bryson's primary interest is advancing "cyber" to integrate with the warfare domains.

Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point and completed numerous U.S. Army professional education courses in tactical communications and information assurance. He holds a Master's Degree in Telecommunications Management from the University of Maryland and a Master's in Business Administration from the University of Florida in addition to completing graduate studies in Electrical Engineering and Computer Science at the University of Texas.

Why a half-life? Because our well-established enterprise computer architecture positions the securityecosystem's primary solution as a kernel-level or Ring 0 module. At Ring 0, the module theoretically has complete visibility and access that software can have on a computer. Threads, hardware access requests, and memory are all managed here. So any general user-mode malware attempting malicious behavior would be identified and handled when it pursues access beyond the established parameters. This concept is architecturally sound.

Reality says otherwise. While the kernel is the logical place for a defense solution to deploy, maintaining kernel stability requires that the module operates predictably. That means it has to be in the same place(s) every time. And that creates vulnerability. Once an intrusion detection technology reaches the tipping point of industry saturation, attackers take notice and work to exploit its predictable location. It simply becomes part of their development and test matrix. As malicious code deploys, the security module is avoided, disabled, or deceived by the intruding exploit.

Take antivirus, for example. Fifteen years ago it was the starting point for staying safe on your computer. Antivirus followed the classic example. Acting from the kernel, an antivirus program had full system visibility and thereby prevented the wrong things from occurring. Initially, these programs looked for malicious signatures, but as attacks became more sophisticated and complex, products were bolstered to identify malicious behaviors. Before long, antivirus technology was widely adopted, becoming the de facto ante for hackers to get onto a computer, and giving rise to industry giants like Symantec and McAfee. Vendors followed the same defensive approach because of the architectural tradeoffs, and as a result, they became vulnerable to the same flaws.

The ubiquity of antivirus solutions quickly challenged bad actors to find innovative ways of defeating them. Reverse engineering antivirus products ultimately revealed their predictability in regards to the kernel-mode security module, enabling attackers to work around a known constant and try successive penetration tactics until something worked. Symantec and McAfee got solved. The ante was met. The paradigm was established.

Hackers work to manage the “eyes”. It’s an eventuality. The solution resides outside of software’s vulnerability. That is not going to happen. Such an approach is just too difficult, too expensive, and too resource-intensive to be practical. Thus we continue to build based on a foundation of what is intrinsically weak.

The one place an attacker is vulnerable is the network. As malware transits the established network infrastructure, it is harder for it to observe defender sensors and relies primarily on stealth. If you have a network tap, it cannot see it; if you have a transparent traffic manager, it cannot see that either. Its best chance at successful exploitation is attempting to innocuously blend in with other network traffic. Although identifying bad traffic from good is a complicated problem, many are trying to solve it. How successful that will be is unknown today. There is, however, one caveat to the network being a kind of safe haven and that is during instrumentation, even network devices are vulnerable to compromise.

Aside from network-level detection, hackers are only caught if they make a mistake, or if there is an environmental change that causes their malware to function outside of developed parameters. Malicious code must be precisely tailored to achieve its aims—it’s like a thread through a needle, traversing a tightly woven computer fabric, but causing the computer to work in a way it was not designed. If there is a change to that “needle,” the thread will miss such that it likely tips off a defender. For example, experiencing multiple Blue Screens of Death would undoubtedly trigger an investigative follow-up that would lead to the discovery of the instigating malware. But this does take time. There is an average of 206 days from breach to discovery.<sup>[1]</sup>

There are those who see machine learning (ML) and artificial intelligence (AI) as potential solutions to the pitfalls of predictable implementations. While ML and AI are enhancements that enable better data analytics, the fundamental data veracity and feature-selection is still questionable. How can you analyze what you never saw in the first place?

Consider how this works. Products incorporating ML are supervised: Someone curates the rules in the vendor’s offline environment that will be pushed to the products. The curation will reduce both false positives and false negatives if done correctly. But this implies that the system only detects anomalies within the range for which it was designed.

On the attacker’s side, new security products incorporating ML and AI are easily added to his or her testing cycle. The malware is validated against the test matrix, ensuring no tested product detects it.

## THERE IS NO CYBER DEFENSE

For now, we have consigned ourselves to perpetually shifting quicksand when we need firm ground to build on. Recognize that. Understand the root cause. Suck it up. New intrusion prevention products may offer temporary relief, but just as a drunk man looks for his keys where the streetlight is already shining, staying in our comfort zone is not going to solve this problem.

Like death and taxes, exploitation is a certainty in life, so the cybersecurity focus should be on detection and response. Reducing the initial scope helps figure out what you've got that matters, then circle the wagons around your crown jewels to protect and control what you can. 🛡️

## **NOTES**

1. 2017 Ponemon Cost of Data Breach Study, <https://www.ibm.com/security/data-breach>.



# Countering the Cyber Threat

---

Shawn Henry

Dr. Aaron F. Brantly

## ABSTRACT

**T**he current path to national cybersecurity hides a fatal design flaw. Resident within the current national approach is the assumption that we can continue business as usual with limited sharing between the public and the private sector, the creation of information sharing and analysis centers, the National Cybersecurity and Communications Integration Center, and a range of ad hoc local, state and federal organizations each addressing a slice of a complex and highly interconnected environment. The result is a lack of integrated coordination, continued hacks, and a public increasingly weary of all things cyber. We are approaching the current challenge as if we are living in August of 2001, ignorant and oblivious to the tragedies just over the horizon. All the while the private sector treats each incident in isolation, highly focused on their slice of a broader digital ecosystem.

In the aftermath of the 9/11 attacks, Congress, the executive agencies and departments, and the judicial system in coordination with the will of the American people moved swiftly on legislation and strategies to address a complex asymmetric threat. While many of these new pieces of legislation failed in the courts, the unity of effort and the subsequent cooperative environment across all levels of government, and with the private sector, have arguably altered the national security posture and environment within the United States. Most of these changes have created a safer and more resilient domestic environment that has largely been spared the ravages of foreign-inspired terrorism. While not perfect, the current approaches adapted through years of learning, information sharing, and practice have safeguarded the homeland in an increasingly dangerous world. Lessons from the last 16 years of countering terrorism (CT) should serve as a roadmap for developing a robust, whole-of-society approach to safeguarding the homeland against the threats emanating from cyberspace looming beyond view.

© 2017 Shawn Henry, Dr. Aaron Brantly





Shawn Henry is the President of CrowdStrike Services and CSO and a retired executive assistant director of the FBI. Henry, who served in three FBI field offices and at the bureau's headquarters, is credited with boosting the FBI's computer crime and cybersecurity investigative capabilities. He oversaw computer crime investigations spanning the globe, including denial-of-service attacks, bank and corporate breaches, and state-intrusions. He posted FBI cyber experts in police agencies around the world, including the Netherlands, Romania, Ukraine and Estonia. He has appeared on "60 Minutes," "CBS Evening News," "Good Morning America," "The Today Show," "Dateline," "Rock Center with Brian Williams" and C-SPAN. He has been interviewed by Forbes, BusinessWeek, The Wall Street Journal, the Associated Press and USA Today.

Henry earned a Bachelor's degree in Business Administration from Hofstra University and a Master's degree in Criminal Justice Administration from Virginia Commonwealth University.

As we move to address the complex cyber environment with nearly one hundred percent Internet saturation,<sup>[1]</sup> 20 billion internet-enabled devices,<sup>[2]</sup> and a world controlled by industrial control systems (ICS), big data,<sup>[3]</sup> machine learning<sup>[4]</sup> and more we must ask ourselves what lessons can we draw from the CT community? We argue for a concerted national effort at every level of government and within the private sector. Below, we outline the fundamental challenges facing the United States and Western Democracies and provide a measured approach for advancing a coordinated effort to safeguard the underpinnings of modern society.

### ***The Evolving Complexity Problem***

It is a bit hard to fathom just how far we have progressed in the 25 years since Congress passed the Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g) when NSFNET was permitted to interconnect and support access to non-educational networks. Although most trace the history of the Internet back to Donald Davies' or Paul Baran's conceptualization of packet switched networks or perhaps to Vint Cerf or Robert Khan who devised TCP/IP, the Internet became truly global when legal barriers to interconnection began to fall away first in 1992, and then again as the restrictions on cryptography began to dissipate between 1992 and 2000 allowing for secure transactions to occur. In 1994, just over 11% of Americans were connected to the Internet, 23 years later more than 87% are connected.

The number of connected devices per American has also grown rapidly as individuals have purchased everything from personal computers to tablets and phones. As the citizenry have increasingly connected to the Internet so to have the businesses, utilities, and governments upon whom they depend daily for commerce, healthcare, banking, education, electricity, entertainment and so much more. What



Dr. Aaron F. Brantly is Assistant Professor of Political Science, Virginia Polytechnic and State University and Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combatting Terrorism Center at the United States Military Academy. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University.

Dr. Brantly has worked on issues related to cybersecurity from multiple angles including, human rights and development, intelligence and national security and military cybersecurity. His interests span the political science and computer science divide. He is currently working on a year-long project on cyber deterrence funded by OSD Minerva R-Def. For further information, please visit [www.afterwestphalia.org](http://www.afterwestphalia.org).

once was a network of academics and researchers has spread to touch every aspect of life.<sup>[5]</sup> Our credit card purchases are monitored based on amount, location, time of day, and frequency for fraud analysis, our power grids balance the load for entire swaths of the nation, our financial markets shift trades around the world in new patterns based on algorithms designed to derive profits from hundredths of a percent change in value. We are conditioned to think of each of these things, these experiences within our daily lives as discrete events, discrete systems, but the reality is far different. We are rapidly advancing towards what William Gibson, the progenitor of the term Cyberspace referred to in fictional terms as a “consensual hallucination.”

This modern connected environment is on a trajectory that will only lead to the increasing proliferation of Internet connected devices and general interconnectivity of nearly every aspect of every individual's daily existence. Because each of the systems within this evolving ecosystem is managed by a different company, government, or individual, each addresses the problems at their level of interaction or occasionally within their sector. The efforts to share information more broadly have been met by distrust of government, legal, financial and business concerns and an onslaught of attacks that overwhelm all but the most well-funded information security operations at major corporations or in the Department of Defense.<sup>[6]</sup> The cybersecurity challenge is multifaceted and decentralized with criminal and state actors spread around the globe.<sup>[7]</sup> A distributed cyber network structure is in many ways similar to the evolving nature of networked terrorism.<sup>[8]</sup> While the volume and spread of nodes within the cyber context are likely more voluminous, the reach and scope of terrorism into state and criminal networks<sup>[9]</sup> is not significantly different than the spread of cybercrime, cyber espionage and cyberattack capabilities across a range of actors.

On September 12, 2001, the problem of transnational terrorism loomed large, and the capacity of international partners, federal, state, local authorities, financial institutions, and a variety of organizations to deal with a complex problem was virtually non-existent.<sup>[10]</sup> Beyond recognizing the problem of terrorism, it was abundantly clear that actors across all levels and within multiple sectors needed to learn to communicate, plan, organize, and react to problems in near real-time. The military, the intelligence community, law enforcement and first responders needed to develop both endogenous capacity and the ability to communicate, strategize and rapidly respond to events. These skill-sets and the technical tools to make them viable were not in existence in September 2001. Yet, today a network of fusion centers, building on the lessons of 9/11, Hurricane Katrina and other significant events have learned to contain and manage crises. The problems posed by cyber threats are unique, in that the technical capacity to respond at both the scale and speed necessary requires many of the same structural and human capital developments to be addressed at a wide range of levels and across a multitude of institutions. In this way, terrorism provides a roadmap for technical and human development to address the cyber challenge now facing the United States.

### ***Solving the cyber problem by planning for it***

Responding to a problem in real-time requires utilizing the tools available. Yet, because the cyber problem is evolving and changing as more and more devices come online, it is better to flip the equation. Assuming a 9/11 scale event against the United States in the future, what tools would the US government, state and local authorities need, what resources could be made available to not one, or two, but dozens of industries simultaneously? What communicative and technical capacity is required at every level, and within each organization to contain a considerable crisis?

First, to advance cybersecurity, there needs to be a consensus across the public and private sector. Consensus must occur both within the United States, and internationally within the community of nations. Great strides have been made to achieve international consensus through the United Nations Group of Governmental Experts (UNGGE).<sup>[11]</sup> The U.S. Department of State has been instrumental in pushing forward key normative issues within the broader international community. Moreover, NATO member countries are slowly moving towards consensus on the urgent need to address cybersecurity.<sup>[12]</sup> NATO member countries have also begun to incorporate critical infrastructures into the discussion on the future of cybersecurity through the NATO Industry Cyber Partnership.<sup>[13]</sup> Other key initiatives include the Budapest Convention on Cybercrime which advances a consensus related to criminal activities within cyberspace. Each of these steps at the international level fosters increased understanding and in the case of NATO communications—how to address significant cyber events.

The United States made strides at the federal level under the Obama administration to create information sharing and analysis organizations, strengthen information and analysis centers<sup>[14]</sup> and manage the federal response to significant cyber incidents under PPD41.<sup>[15]</sup> Many of these coordination and management improvements have advanced a more robust and unified domestic approach to national cybersecurity in tandem with advances in military cybersecurity development that began in the mid-2000s and began to rapidly increase in speed in 2010 with the creation of U.S. Cyber Command. Yet, despite sweeping organizational changes, cybersecurity within the Federal government remains both complicated<sup>[16]</sup> and poorly implemented with continued significant intrusions into government networks.<sup>[17]</sup>

Below the federal level, most states and larger cities are only now just beginning to develop internal cybersecurity capabilities, while most counties and local municipalities have long been woefully ill-equipped to deal with a cyber domain that is quickly facilitating and encompassing larger portions of their information management procedures and constituent services delivery.<sup>[18]</sup> Many of the issues that plague the Federal government are more pronounced at the state and local level, namely human capital and coordination between actors.

Whereas in the aftermath of 9/11 there was a rapid movement across all levels of government to train and equip state and local authorities to manage significant terrorist crises, the same urgency is lacking in response to reoccurring cyber incidents. The scale and frequency of damage caused by cyberattacks against federal, state and local entities is substantial. Recent years provide a plethora of events in which courts, local governments, or mass-transit systems have been substantially impacted by cyberattacks.<sup>[19]</sup> While the recognition of the enormity of the problem is slowly being realized, the speed with which state and local actors are addressing these issues leaves millions of individuals, and thousands of firms and governments vulnerable.

Outside of government, private sector problems associated with cybersecurity are extensive but stratified across thousands of industries, sizes and types of firms, each with differing levels of capacity to address an ever more complicated threat environment. Although terrorism affected businesses and their operational plans, not all businesses and firms were necessarily affected by terrorism to the same extent that each company is vulnerable to cyberattacks. Specific industries such as aviation, banking, and utilities among others were directly affected and required to implement new security measures, monitoring of accounts and take other precautions; generally, the threat environment was more constrained than it is presently in cyberspace. By contrast, the impact of cyberattacks on one industry can rapidly cascade and affect other industries, most recently demonstrated by the NotPetya and WannaCry attacks of 2017.<sup>[20]</sup>

Cybersecurity is currently fragmented. Each actor acts mainly alone or with limited connections to other entities within their industry and varying government interactions. It is imperative that we continue to build consensus around the problems associated with cybersecurity at every level. It is only when there is a universal recognition of the cyber challenge that as a nation we can focus our efforts on the second and third critical tasks that must occur to foster cybersecurity nationally.

Upon the development of consensus, the second facet of addressing the cybersecurity problem is the creation of a tightly interwoven information and communications network that provides rapidly declassified and anonymized threat indicators to halt the spread of malware, quickly detects emerging attacks, and enables attribution. The third undertaking is the sustained development of the human capital necessary to develop, understand, and respond to these threat indicators. These indicators are early warnings of imminent events. Presently, the classification of data, legal, financial or other concerns regarding the dissemination of information delay the development and transmission of this information, complicating the responses of corporations and governments across all ecosystems. Businesses and government agencies should be incentivized to engage in information sharing with assurances that the data being provided will not end up classified or used to adversely affect their firm or government as long as gross negligence or criminal acts did not occur. Trust within an ever-expanding, and resilient information and communications network for cybersecurity is of critical importance and should be incentivized at every level of government and across the private sector. Upon receipt of threat indicators, it is imperative that each entity has the necessary minimum qualified personnel to address the threat to their firm and prevent its spread to other companies within its ecosystem.

Fourth, building on information sharing networks and trained personnel is a need to develop robust public-private, cross-firm, and cross-industry liaison networks. Such networks would serve to minimize localized thinking in threat response and help firms and governments act more broadly by understanding cross-firm-sector-government challenges. By understanding these challenges and addressing how defensive or offensive actions in one industry affects others, the intent is to create a network that responds through a unified effort that minimizes systemic problems and their impact not only within a single firm but across entire sectors. Liaisons have been beneficial to the post-9/11 counter-terrorism efforts and would most certainly be of benefit to addressing cybersecurity challenges.<sup>[21]</sup>

Fifth, cybersecurity is a team sport. It is not isolated to one company, one sector, or one type of government but crosses boundaries between and amongst them. Shifting the focus from a one-off company or government protection to a more holistic team-based approach will increase the aggregate resilience of the nation. Likewise, while the short-term

costs incurred in developing the structures and processes above are likely to be high, the efficiency gains and savings through the avoidance or minimization of risk are expected to result in net benefits. Where firms or governments are too small to adequately provide protection independently, they would benefit from liaison relationships and cybersecurity coordination with larger firms within the same or similar industries. The larger firms or governments might not see an immediate benefit to providing support to smaller entities, but in providing support to less capable allies, they defend their networks against potential vectors of attack.

Cybersecurity is complex, and the structures and processes articulated in this section are oversimplifications. The process by which the nation responded to the threat of terrorism provides a pathway for developing the reforms necessary to address the cybersecurity problem. Through consensus, planning, and coordination, the United States can begin to take the independent actions of diverse groups and provide a unity of effort to advance cooperative security. This more effective and efficient environment is a foundational step necessary to create a safer and more resilient nation better able to address the cybersecurity problems of the present and into our future.🛡️



## NOTES

1. <http://www.internetworldstats.com/america.htm#us>.
2. Amy Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated." *IEEE Spectrum*, August, 2016.
3. Paul Burkhardt, "An Overview of Big Data." *The Next Wave* 20 (4): 2014, 1–47. <https://www.nsa.gov/research/tnw/tnw204/article1.shtml>; 2014. "Big Data: Seizing Opportunities, Preserving Values." Executive Office of the President.
4. "Big Data: a Report on Algorithmic Systems, Opportunity, and Civil Rights." Executive Office of the President, 2016.
5. Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Decision-making*. University of Georgia Press, 2016.
6. Andrew Nolan, "Cybersecurity and Information Sharing: Legal Challenges and Solutions." 7 ed. Washington: Congressional Research Service, 2015; Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing." *Military and Strategic Affairs* 6 (3), 2014; Steven P. Wittenberg, "When to Disclose Data Breaches Under Federal Securities Laws," *Illinois Business Law Journal*, October, 2016, "2016 Financial Industry Cybersecurity Report." [https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard\\_2016\\_Financial\\_Report.pdf](https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf).
7. United States Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity and Security Technologies, *Emerging Cyber Threats to the United States*. 114th Cong. 2nd sess. Washington: GPO. 2016; (Statement of Frank J. Cilluffo Director, Center for Cyber & Homeland Security at George Washington University).
8. Marc Sageman, *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2011.
9. Scott Helfstein and John Solomon, "Risky Business: The Global Threat Network and the Politics of Contraband." Combating Terrorism Center at West Point, 2014.
10. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Government Printing Office: 2004, 16–419.
11. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." A/70/174. New York: U.N., General Assembly, 2015. [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
12. [http://www.nato.int/cps/en/natohq/topics\\_78170.htm](http://www.nato.int/cps/en/natohq/topics_78170.htm).
13. <http://www.nicp.nato.int>.
14. Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing, <https://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf>.
15. Presidential Policy Directive 41 -- United States Cyber Incident Coordination <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
16. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Gao. Gov. Washington, 2013; Richard Bejtlich, "What Are the Prospects for the Cyber Threat Intelligence Integration Center?," Brookings, Washington: February 19, 2015. <https://www.brookings.edu/blog/techtank/2015/02/19/what-are-the-prospects-for-the-cyber-threat-intelligence-integration-center/>.
17. *Federal Information Security Modernization Act of 2014: Annual Report to Congress Fiscal Year 2016*, Whitehouse.Gov, Washington, 2017.
18. Jim E. Crouch and Larry K. McKee Jr., "Cybersecurity at the State and Municipality Levels: Where Do We Stand?," National Security Cyberspace Institute, February 25, 2011, <http://www.nsci-va.org/WhitePapers/2011-02-25-State-Municipality%20Cybersecurity-NSCI-Crouch-McKee.pdf>; Richard Clarke and Karen Jackson, "Commonwealth of Virginia Cyber Security Commission First Report, August 2015: 'Threats and Opportunities'," Commonwealth of Virginia.
19. James Scott and Drew Spaniel, "ICIT Ransomware Report." Institute for Critical Infrastructure Technology, 2016; Jack Stewart, "SF'S Transit Hack Could've Been Way Worse—and Cities Need to Get Ready," *Wired.com*. November 28, 2016, <https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare/>.

## NOTES

20. Karan Sood and Shaun Hurley, “NotPetya Ransomware Attack Technical Analysis: a Triple Threat: File Encryption, MFT Encryption, Credential Theft,” *CrowdStrike.com*, June 29, 2017, <https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>; Adam McNeil, “How Did the WannaCry Ransomworm Spread? - Malwarebytes Labs.” *Blog.Malwarebytes.com*. May 30, 2017, <https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/>.

21. Daniel Byman, “Intelligence Liaison and Counterterrorism: A Quick Primer.” *Lawfare*. May 16, 2017, <https://www.lawfareblog.com/intelligence-liaison-and-counterterrorism-quick-primer>.





# The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace

---

Elad Yoran

Edward G. Amoroso

## ABSTRACT

Commercially-available, end-to-end encryption software application solutions address cyber threats from advanced nation-state actors by securing mobile voice communications from eavesdropping. Existing mobile security frameworks, such as explained in a recent Department of Homeland Security (DHS) study, provide a good base for analysis, but are shown to have dealt insufficiently with the threat to mobile voice and corresponding encryption-based safeguards. A secure cyberspace thus requires increased attention to securing voice in addition to data when using mobile devices.

## INTRODUCTION

During the Vietnam War, the National Security Agency (NSA) supported a tactical secure voice system called NESTOR,<sup>[1]</sup> which was used for communications between American warfighters. NESTOR equipment was bulky, often requiring a large man-pack. To make a secure call, the operator had to work through a series of complex keying options using a mechanical loader with a matrix of switches. Once connectivity was established, voice quality using this secure voice scheme was generally poor.

Fast forward to modern civilian, industrial, and military contexts, and one finds a variety of improved options for secure voice. The warfighter, for example, has access to customized Command, Control, Communications, Computers, and Intelligence (C4I) systems with rugged ergonomics and support for secure voice using special radios that offer location, texting, and related real-time data. These radios are typically tailored for military use and built to the specification of the warfighter (see<sup>[2]</sup>, for example).

In addition, however, modern users of mobility in both military and non-military contexts now have access to secure end-to-end voice options using familiar, commercial off-the-shelf (COTS) solutions available on smartphones made by the likes of Samsung



Elad Yoran is Executive Chairman of KoolSpan and CEO of Security Growth Partners (SGP). He is a 20+ year cybersecurity veteran, among other things having founded and led many foundational cyber start-up companies. He was honored as “Entrepreneur of the Year” by E&Y. Elad’s cybersecurity entrepreneurial experience includes Riptech, acquired by Symantec; Medi-aSentry, acquired by SafeNet; Sentrigo, acquired by McAfee; and Vaultive. Previously, Elad served as VP Global Business Development at Symantec. In addition, Elad was a strategic investor and advisor to Red Owl Analytics, acquired by Forcepoint; NetWitness, acquired by RSA; ThreatGrid, acquired by Cisco; and Insightix, acquired by McAfee.

He serves as director at Infinidat. Elad also serves on several government and industry boards. He is an advisor at the Army Cyber Institute, director of the Cloud Security Alliance, and previously, the FBI IT Advisory Council. Elad is the author of many cyber articles going back to the original Internet Security Threat Report research papers. Previously, Elad served as a US Army officer and is a graduate of the Wharton School and West Point.

and Apple. While one would not expect pure COTS to supplant tailored military voice applications, cybersecurity practitioners have come to recognize that cyber threats from nation-states and others extend far beyond traditional military and government organizations, and target commercial businesses for valuable IP, trade secrets, business strategies, negotiating positions, and more. Corporate espionage executed via interception of mobile communications is a growing global phenomenon.

As one might expect, mobility is a direct target in such contexts—and this includes the plethora of ecosystem components used to support mobility services. To this end, the DHS recently issued a technical report in conjunction with the National Institute of Standards and Technology (NIST). With the simple title: *Study on Mobile Device Security*<sup>[3]</sup>, the report offers a thorough overview of issues in protecting mobile devices and systems from cyber threats across a range of individual, corporate, and government scenarios.

While the DHS study offers a thorough description of general mobile security, we believe that its emphasis on secure mobile voice is insufficient. Such oversight is indicative of a larger trend where protection of voice communication is often ignored by security engineers designing modern cyber defenses. With growing cyber threats to communications using mobile devices and infrastructure, increased focus in this area will help safeguard the use of mobility across all aspects of cyberspace.

### ***General Model of Secure Mobility***

A significant contribution of the *Study on Mobile Security* is that it offers a clean model of the commercially-available mobile ecosystem—one that we recommend as the canonical default for anyone trying to make a claim or technical point concerning any aspect of mobile security, including outside



Dr. Edward G. Amoroso is Chief Executive Officer of TAG Cyber LLC, a global cyber security advisory, training, consulting, and media services company supporting hundreds of major organizations across the world. Ed recently retired from AT&T after thirty-one years of service, beginning in Unix security R&D at Bell Labs and culminating as Senior Vice President and Chief Security Officer of AT&T from 2004 to 2016. He was elected an AT&T Fellow in 2010.

Ed has been Adjunct Professor of Computer Science at the Stevens Institute of Technology for the past twenty-nine years, where he has introduced over three thousand graduate students to the topic of information security. He is also a Research Professor in the Computer Science Department at the NYU Tandon School of Engineering, and a Senior Advisor at the Applied Physics Laboratory at Johns Hopkins University. He is author of six books on cyber security, and dozens of major research and technical papers in peer-reviewed journals and conference proceedings.

the United States. Below, we redraw the model with more generic icons and connections; readers are encouraged to use this simple base to instantiate a more tailored local enterprise view.

The components of the DHS mobile ecosystem model include the five main commercial components of government, enterprise, and consumer mobility: *Mobile devices, mobile apps, mobile operating systems, enterprise mobility management (EMM), and mobility networks*. These components form the base on which further cybersecurity investigation to minimize mobile risk can be performed. The DHS study does an admirable job in this regard for general threats to mobility for mobile data, mobile Internet, and mobile app usage.

Mobile devices and operating systems, for example, are shown to require considerable security regarding their design and operation. The device technology stack is shown to create opportunities to harden devices from advanced cyberattacks. Mobile apps made available from mobile app stores are also shown in the DHS study to offer opportunities for improved security, as are EMM systems, common in modern businesses.

The study also explains the challenges of mobile network infrastructure in dealing with attacks. It introduces a threat taxonomy that operators and users of modern WiFi, 2G, 3G, 4G, LTE, and emerging 5G networks must contend with, as they use commercially obtained mobile devices to accomplish their mission—whether business or entertainment-related. The report does not, however, adequately cover the threats or corresponding solutions for supporting secure mobile voice. The remainder of this paper is designed to fill in that gap.

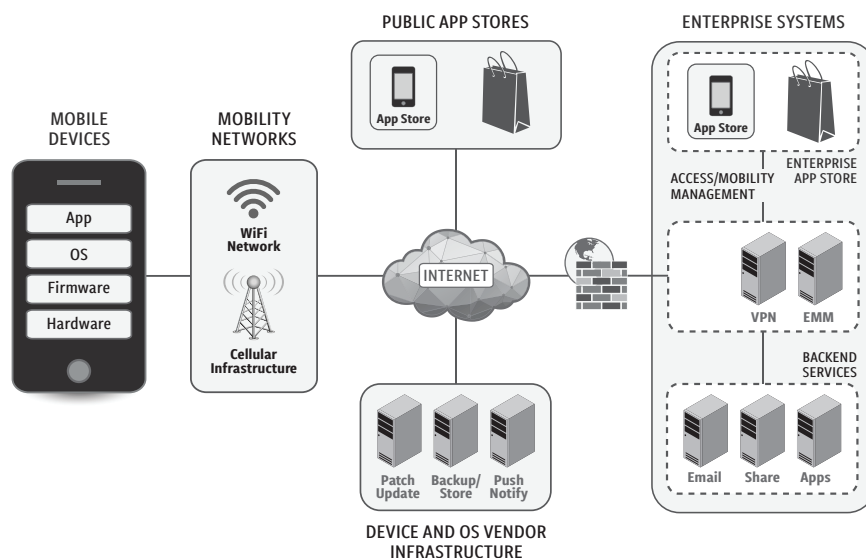


Figure 1. Generic DHS Mobile Ecosystem Model

### Threats to Mobile Voice

The obvious threat to mobile voice is an eavesdropper listening to conversations for purposes that can range from military tactics to corporate espionage. For many years, security engineers have drawn the proverbial diagram showing Alice and Bob communicating end-to-end, with Eve positioned as an active man-in-the-middle adversary, collecting targeted communications from network media, and then analyzing and interpreting the content. In the early days of voice, this was done using simple wiretaps on circuit-switched lines.

One might have expected that with the advent of packet-switched voice communications such as Long Term Evolution (LTE), that mobile voice wiretapping would be no longer feasible. Internet packets, after all, are scattered across networks, which would seem to imply that adversaries with wiretap equipment would no longer have an easy time clamping onto a circuit to listen. The reality, however, is that many reasonable options still exist for modern mobile voice communications to be eavesdropped by third-parties.

The most commonly cited example of mobile voice interception by an adversary is the so-called *IMSI catcher method*<sup>[4]</sup>. Each mobile network operator (MNO) supports a non-secret individual mobile subscriber identifier (IMSI) that allows for differentiation between mobile end-users. The idea of an IMSI catcher attack is that a fake base station is placed proximate to the intended surveillance target. Since earlier generation mobile technologies including 2G services do not include tower authentication by the base unit, any device using such technology—and this includes popular fallback services for coverage—will be tricked to connect to the fake station.

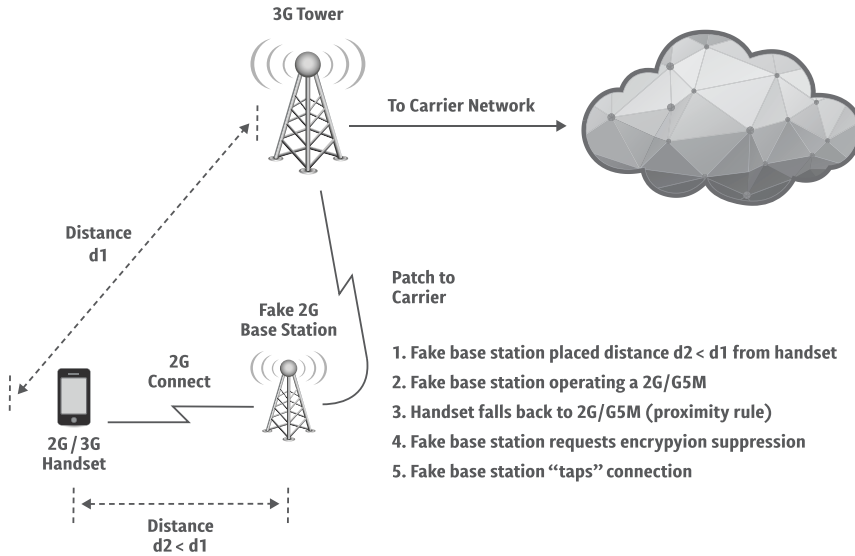


Figure 2. IMSI Catcher Concept

The result of this tactic is that the interceptor can collect all transmitted communications, such as a voice conversation, and through directed, suppressed encryption, can perform a wiretap. IMSI-based surveillance is prevalent today, including use by law enforcement organizations at Federal, state, and local levels. While they generate a fair amount of media attention and legal debate regarding the constitutionality of how IMSI catchers are used, over time, with most MNOs retiring older technologies in lieu of more secure mutually authenticated and encrypted protocols, this surveillance technique should be less of an issue. But it illustrates effectively the types of security problems that emerge in any complex mobile infrastructure setting, and it underscores the importance of security vigilance by the mobile carrier.

An additional and far more widespread and long-term threat to secure mobile voice involves the mobile network infrastructure. Core mobile network operation in the DHS report, for example, is recognized as having "virtually unlimited options and attack vectors." This has traditionally involved denial of service and other attacks on infrastructure, but more recently has involved weaknesses in the legacy Signaling System 7 (SS7) protocol, used for the past three decades as the global signaling standard for public switched telephony, which continues to support a large portion of mobile traffic.

SS7's designated successor, the Diameter protocol, supports similar functions. While Diameter is designed to be more resistant to attack, the Federal Communications Commission (FCC) claims that it could introduce new vulnerabilities that need to be considered. From an FCC report, the claim is made that "the two protocols work very differently as do their network substrates and systemic effects, and this should be taken into consideration when assessing Diameter. That said, the research community has given demonstrations

using the Diameter protocol to execute similar exploits seen on the SS7 network. Also, researchers have identified other potential, theoretical exploits on Diameter.”<sup>[5]</sup>

From the perspective of secure voice services, the primary concern regarding SS7/Diameter is the purported possibility of a man-in-the-middle eavesdropping threat, which can include direct wiretaps of conversations by untrustworthy mobile network operators. As described in the DHS study, these threats have been demonstrated in numerous cases including by German researcher Tobias Engel<sup>[3]</sup>. According to the DHS report, “Gaining unauthorized access to the core SS7 or Diameter network is a risk since there are tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage.” While direct access to SS7 has been assumed to be a pre-requisite, several scenarios have emerged with indirect access via femtocell or other equipment.<sup>[6]</sup>

Another consideration regarding this threat is the national economic threat posed by corporate espionage, especially in places where traveling business executives find themselves where the mobile network operator might be largely unconstrained regarding the SS7-based operation. This results in the unusual situation where the modern traveler experiences the type of threat pressure previously experienced by warfighters in foreign battlefields. Corporate IT Security teams deal with this problem through policies that prevent executive travel into certain regions with their mobile devices<sup>[7]</sup>.

### ***Commercial End-to-End Encrypted Calling***

Users of mobility who are concerned with the mobile voice threats posed by IMSI catchers or signaling vulnerabilities—especially in cases where the mobile services are being offered in a geographic region with less robust security—should immediately consider the use of an over-the-top encrypted voice solution. This end-to-end risk mitigation makes perfect sense for the modern, traveling business executive. It also makes sense for anyone—including military personnel—who are concerned with secure voice protection.

The primary functional requirement for secure, end-to-end encrypted voice capability is that it operates independently of underlying mobile network operations. That is, over-the-top (OTT) security is a critical need if existing (or future) vulnerabilities in the network infrastructure could undermine confidentiality demands. This requirement also implies that the encryption support is enabled in proximity to the actual human voice, which suggests that end-to-end encryption becomes a client-enabled function embedded in the mobile device.

Due to this mobile endpoint emphasis, second-order functional requirements emerge to support secure end-to-end mobile voice. First, the end-user should not have to engage in complex administration such as manual keying. Instead, the secure mobile solution should make it simple for end-users to engage in encrypted calls without any specialized training. Second, the end-to-end solution must integrate with modern devices and services. In the



military, for example, as in the commercial world, it is impossible to separate the war-fighter, corporate executive, or traveling business person from their iPhone and Android devices. They have become ubiquitous, and the convenience of voice calling, mobile app use, and Internet access have overshadowed threats targeting governments, business people, and citizens.

The overall functional schema for end-to-end secure mobile voice using commercially available devices and network services are shown in Figure 3 below. The administration and set-up of this capability are not shown on the diagram, but would likely follow procedures consistent with the procurement and use of any commercial capability such as buying and enabling an iPhone from an Apple store. This is an essential point because different products will have different administrative procedures for distribution, maintenance, and support (see <sup>[8]</sup> as an example of one provider's approach).

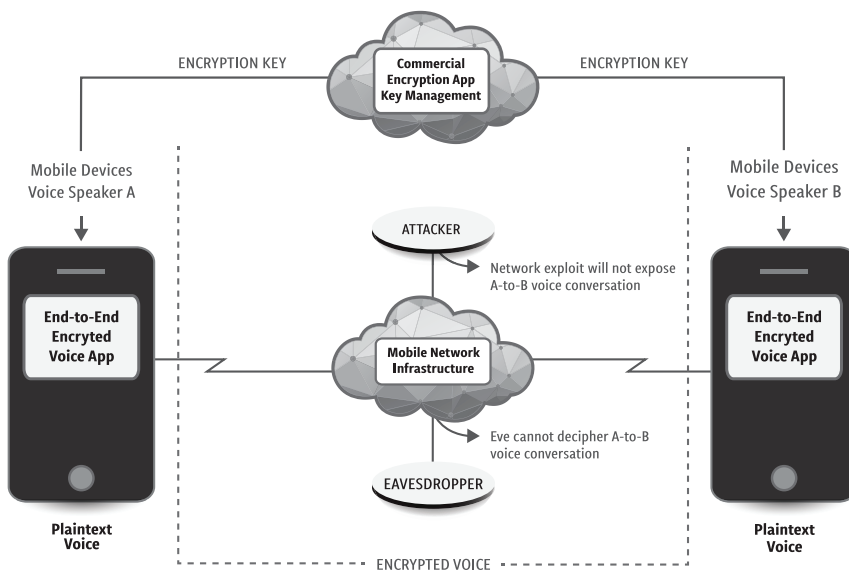


Figure 3. End-to-End Secure Encrypted Mobile Voice

This simple encrypted mobile voice set-up is surprisingly resilient against most modern cyber threats. Certainly, modern mobile communications would not be protected from massive destructive or denial-of-service attacks against the underlying network infrastructure; the provision of end-to-end encryption for voice deals with the disclosure issue primarily. In addition, this end-to-end solution using commercially available encryption would likely not be a robust option in cases where the adversary is likely to employ the most advanced forms of nation-state sponsored cryptanalysis. Tailored military encryption with the proper certifications would be best in these cases.



To the degree, however, that the modern virtual battlefield in cyberspace includes citizens, consumers, businesses of all sizes, civilian agencies, and military organizations—and this extends to all nations, the use of commercially available, end-to-end encryption solutions for mobile voice is both effective and recommended. As the DHS study called for end-to-end encryption for all communication paths, one would hope that national initiatives would be championed at the senior-most levels of government to drive this point. Everyone should be encouraged to make use of secure mobile voice, perhaps even as a casual matter of normal voice communications. With such senior emphasis, one might expect that future DHS studies would focus more on this issue.

## **CONCLUDING REMARKS**

In closing, it is helpful to remember that mobile devices and the supporting ecosystem were originally developed to support voice applications and that this remains a foundational application of mobility. During the past decade, however, most marketing emphasis in mobility has been directed at messaging and mobile application use, rather than voice. We believe, however, as argued in this paper, that the pendulum has swung too far from voice and that mobile security will be better served with more balance between data and voice security.

To help demonstrate the reality of the threat to mobile voice, one might consider that the typical consumer or business person has repeatedly been warned to avoid typing anything into an email or social post that would reflect poorly if posted to the cover of a newspaper. We all know this common aphorism: *If you wouldn't want something printed in the New York Times, then don't put it into an email.* This is sensible advice, and most individuals have tried to adjust accordingly.

An irony, however, is that many sensitive business and personal communications have been shifted from written email to spoken voice, simply to avoid the prying eyes of some man-in-the-middle hacker. This is a good decision in the presence of proper voice security but can be cataclysmic in its absence. Perhaps a new warning should emerge: *If you wouldn't want the transcript of your voice conversation posted to WikiLeaks, then don't say it into your mobile.*

The good news is that with advanced secure end-to-end encryption solutions for mobile voice, the reality is that private citizens, business people, and government officials can make use of their commercially available mobile devices to hold private conversations beyond the reach of an adversary. With the front lines of cybersecurity now extending far beyond the traditional military battlefield, this advance is imperative. By employing such capability, we can all help make cyberspace a more secure environment in which to maintain a safe society. 🛡️

## NOTES

1. [http://www.governmentattic.org/18docs/Hist\\_US\\_COMSEC\\_Boak\\_NSA\\_1973u.pdf](http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf).
2. <https://defensesystems.com/articles/2017/11/cw/navy-darpa-voice-text.aspx>.
3. <https://www.dhs.gov/publication/csd-mobile-device-security-study>.
4. <https://techcrunch.com/2017/06/02/who-catches-the-imsi-catchers-researchers-demonstrate-stingray-detection-kit/>.
5. Federal Communications Commission, *The Communications Security, Reliability and Interoperability Council V Working Group 10 Final Report March 2017*, <https://www.fcc.gov/files/csrc5-wg7-finalreport031517pdf>.
6. <https://www.cbsnews.com/news/60-minutes-hacking-your-phone/>.
7. <http://searchsecurity.techtarget.com/answer/How-to-protect-sensitive-data-when-executives-travel-abroad>.
8. <https://koolspan.com/solutions/>.



# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆



# Smart Bases, Smart Decisions

---

Dr. Harold J. Arata III

Mr. Brian L. Hale

## ABSTRACT

We are living in a time when virtually anything can be connected to the Internet: from smart clothing to autonomous driving to near real-time management of assets in agriculture, manufacturing, logistics, and more—the possibilities are endless. Among this connectedness, the smart cities trend continues to gain momentum. In November 2017, a real estate investment firm owned by Microsoft co-founder Bill Gates announced they purchased nearly 25,000 acres, approximately 45 minutes west of downtown Phoenix for \$80 million for development into a smart community. <sup>[1]</sup> Similarly, Google's parent company, Alphabet, committed \$50 million for a Toronto neighborhood development, AT&T is investing nearly \$3 billion in the Atlanta area to enhance smart-city networks, and Saudi Arabia is forecasting a \$500 billion investment in a mega-city spanning three countries intended to “push the boundaries of innovation.” <sup>[2,3]</sup> A smart base may be able to take advantage of the same benefits anticipated for a smart city, with added military capabilities—mission assurance and mission command.

### *The Advent of the Internet of Things (IoT)*

Technology is revolutionizing life, and it's not slowing down. In 1999, Kevin Ashton, an assistant brand manager at Procter & Gamble, delivered a presentation about wireless connectivity with an intriguing title: “Internet of Things.” Sketching out a futuristic scenario where computers “knew everything there was to know about things as the network connected objects in the physical world to the Internet,” Ashton predicted the IoT “has the potential to change the world, just as the Internet did. Maybe even more so.” <sup>[4]</sup> Almost two decades later, the digital shift Ashton imagined is well underway. Organizations are using the IoT to glean new operational insights, grow revenues, reduce costs, and increase productivity.

©2017 Dr. Harold Arata, Brian Hale



Dr. Harold J. Arata III, CISSP, is the Lead Systems Design Engineer at AT&T, supporting AT&T Government Solutions. Most recently, Dr. Arata served as an Executive for Cybersecurity Strategy at Hewlett Packard Enterprise (HPE), Enterprise Security Solutions. Prior to HPE, Dr. Arata was the Director for a Cyber Center of Excellence at a not-for-profit research institute. Preceding his career in industry, Dr. Arata was selectively nominated and selected as the Director—U.S. Air Force Cyberspace Technical Center of Excellence, Air Force Institute of Technology (AFIT), educating 650 joint cyber professionals a year. Dr. Arata served as a Senior Military Professor at AFIT, conducting defense-focused research at the Master's and Ph.D. levels. Preceding Dr. Arata's federal civil service, he was an active duty 2 year below-the-zone select to Full Colonel. Dr. Arata's military awards include being individually designated Best-in-Air Force as the Lt. General Leo Marque Communications-Electronics award winner and is a recipient of the Legion of Merit.

In the twentieth century, computers were brains without senses—they only knew what users told them. This was a huge limitation: there are many billion times more information in the world than people could type through a keyboard or scan with a barcode. On the other hand, automated and data-powered actions can process 55 trillion measurements per day, and make 1.3 million automated optimizations per day. Similarly, threat detection involved human-managed firewall monitoring and reactive threat responses to over 750 billion events per day. Data-powered actions enable analyzing up to 5,000 events per microsecond promoting a proactive self-healing network fabric.<sup>[5]</sup>

Today, because of the IoT, the number of interconnected sensors has exploded. It's only been a few years; however, this data transformation of networked sensors is already being taken for granted.<sup>[6]</sup> Figure 1, illustrates this remarkable transformation.

Edge intelligence advances this transformation as it pushes processing for data-intensive applications away from the core of the cloud to the edge of the network thereby realizing the real value of the IoT. This radical transformation from the cloud to the edge, 'edge intelligence,' will support trillions of sensors and billions of systems. It will treat data in motion differently from data at rest. By shifting intelligence from a core centralized cloud to a gateway at the edge of an organization's network, sense-making and near real-time decisions can be made closer to when they need to occur. This model reduces the impact on the network by having data crunching and analytics move closer to the edge, with smaller data streams forwarded to the cloud. Edge computing can also help solve latency challenges and enable organizations to take better advantage of opportunities leveraging a cloud computing architecture. Cities and military installations

would be prudent to prepare for disruptions in their business and military models. For example, during the last decade, there has been a change from the traditional software license model to the services model: software as a service, platform as a service, and infrastructure as a service.<sup>[7]</sup>

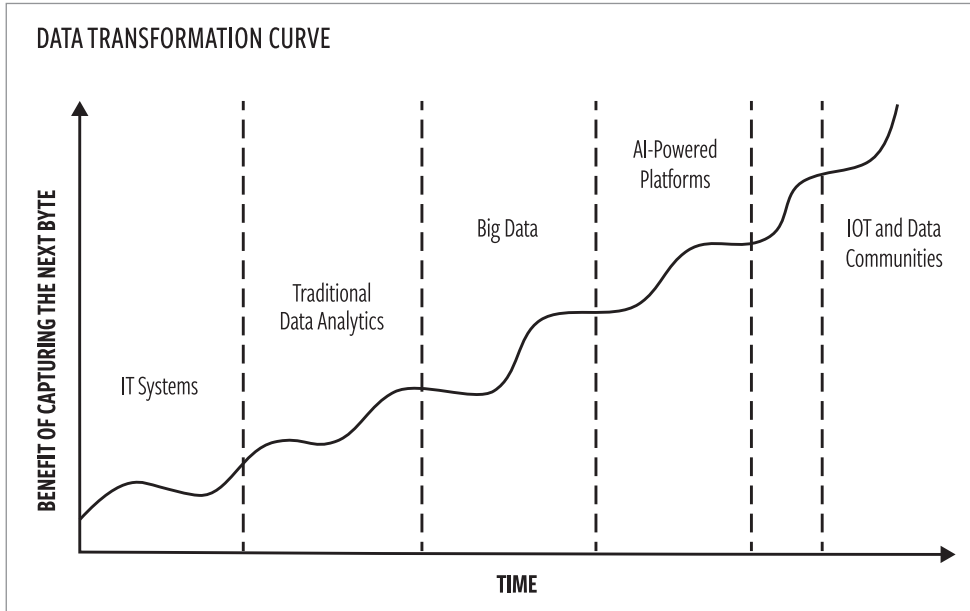


Figure 1. Benefit of capturing the next data byte over time

Furthermore, driven by the IoT, a new computing model is currently evolving, as shown in Figure 2. This extensive ecosystem of interconnected devices, operational tools, and facilities holds much promise for connecting people, processes, and assets in ways profoundly impacting how people live and work. IoT allows organizations to improve everything with data-powered insights.

The impact of this data-powered journey uses advanced analytics to translate vast amounts of collected, raw data into actionable intelligence that a city/base can use to improve the performance of its infrastructure and make long-term cost savings.

### ***IoT Moves to the City***

Cities are facing unprecedented challenges. The pace of urbanization is increasing exponentially. Every day, urban areas grow by almost 150,000 people, either due to migration or births. Between 2011 and 2050, the world's urban population is projected to rise by 72 percent (i.e., from 3.6 billion to 6.3 billion) and the population share in urban areas from 52 percent in 2011 to 67 percent in 2050. Additionally, the increased mobility of our societies has created intense competition between cities to attract skilled residents, companies, and organizations.<sup>[8]</sup>





Mr. Brian L. Hale, CISSP, is a senior Cybersecurity Analyst at HX5. Most recently, Mr. Hale served as the Associate Director for Cybersecurity Strategy at Hewlett Packard Enterprise (HPE), Enterprise Security Solutions. Prior to his work at HPE, Mr. Hale was the Operations Officer for a Cyber Center of Excellence at a not-for-profit scientific research institute. Preceding his career in industry, Mr. Hale was appointed as the Deputy Chief, Cyber Professional Continuing Education Division, Air Force Cyberspace Technical Center of Excellence, Air Force Institute of Technology (AFIT). Mr. Hale also served in the U.S. Air Force and retired in April 2012 after a 26-year career. Mr. Hale earned a Master of Science Degree in Information Resource Management from AFIT, a Bachelor of Science Degree in Management/Computer Information Systems from Park University, and two Associate degrees.

Furthermore, with this increased urbanization, the total number of machine-to-machine connections will grow from 5 billion in 2014 to 27 billion in 2024.<sup>[9]</sup> With this population density increase comes: increased crime, pedestrian safety, and aging infrastructure that cannot handle present population loads. According to America's Infrastructure 2017 report card, in the US there is an estimated \$2.0 trillion needed by 2025 to correct infrastructure deficiencies.<sup>[10]</sup> Similarly, economic development a hot topic for politicians, will likely drive more connected/intelligent cities to attract established companies and perpetuate benefits to stimulate job growth and sustainability. To address these challenges, the concept of the smart city, the integration of technology with a strategic approach to sustainability, cost reduction, citizen well-being and economic development, has been conceived.

***Smart cities are concentrating on a variety of supporting IoT devices in the following areas:***

- ◆ **Public Safety:** the number one priority for many cities is public safety and the quality of life of their citizens. Using sensors and various smart-city technologies, city governments are implementing solutions to provide enhanced public safety to their constituents by delivering enhanced video surveillance at intersections, local parks, and other locations; installing sensors to alert authorities when suspicious activity takes place after hours; setting up license plate scanners embedded in video cameras to identify stolen vehicles; and mounting gunshot sensors on city light posts that immediately report the location of gunfire to first responders.
- ◆ **Infrastructure Monitoring:** city engineers stay remotely connected so they can monitor and measure changes within city structures

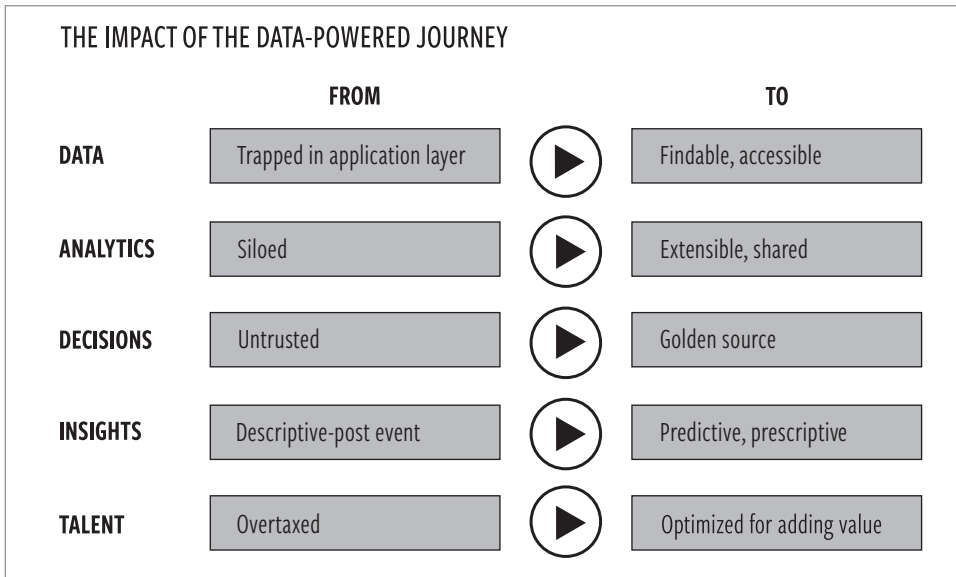


Figure 2. The data-powered journey

or earthworks. This includes an increase in efficiency and connectivity by utilizing connected lighting platforms with automated alerts to promote reductions in city-wide energy costs.

- ◆ **Multi-Network Solutions:** the IoT revolution offers a wide-range of network options to customers that support connectivity from parking meters to farm equipment, and everything in between using a variety of the latest technologies such as cellular (LTE/4&5G); fiber; small cell; low power wide area networks; and satellite communications.
- ◆ **Logistics Management:** city logisticians can shift to condition-based maintenance to improve performance and reduce costs. Employ automation to enhance container visibility across the supply chain. Correspondingly, automated data can simplify orders and reduce emergency deliveries. Similarly, savings on fuel costs through route optimization, minimized idling, and keeping customers informed with real-time to vehicle locations can be realized.
- ◆ **Waste Management:** cities can install and connect sensors in their trash bins, allowing them to receive real-time capacity data to enhance their logistics and waste management efficiencies; thereby providing real-time volume reports to optimize collection routes versus scheduled routes. Likewise, improved monitoring of driver behavior and vehicle conditions; allows for reducing infraction risks and optimizing driver performance.

- ◆ **Water Management:** water usage and sustainability are critical factors to cities. Smart water management is an opportunity to not only conserve but preserve the water supply with advanced sensors to reduce waste. Sensors in the water supply can precisely locate and detect leaks before they become a major issue; allowing for more efficient maintenance and repair. Alerts can also inform an individual or business of abnormal water usage in real time.
- ◆ **Smart Cities Operations Center:** the Smart Cities Operation Center is a data visualization tool that integrates and aggregates various data points and outputs the data in an easy to digest format. The aggregated IoT data is then used by local utilities, chief information officers, and mayors, to track and improve issues and efficiencies in real-time.
- ◆ **Traffic Analytics:** traffic is one of the biggest pain points for cities, and a difficult quality of life indicator to improve. Sensors installed at intersections can identify and alert local municipalities of unexpected traffic or congestion, and dispatch responders quickly and efficiently. Traffic type (pedestrian, bicycle, vehicle) information can be collected in real time offering the city the opportunity to optimize ingress and egress routes for the various modes of transportation. Small business can utilize the traffic analytics data in determining the optimal location to build their next franchise.

These transformations will require radical changes in the way cities are run. Smart cities are necessary to reduce emissions and handle rapid urban growth. Rather than being an expense, smart technology integration can create considerable opportunities for added value in cities of the future.<sup>[11]</sup>

### ***Evolution of Smart Bases***

With the smart-cities movement gaining more traction, and the convergence of the IoT, the successes of smart-city initiatives may be directly applicable to military installations. This extrapolation and enthusiasm are further fueled as technology disruptors shift their focus to relevant smart-city innovations.

“Military Bases function as small cities,” said Colonel Don Lewis, 42d Mission Support Group Commander, Maxwell Air Force Base. “We face a lot of the same challenges municipalities face. We're excited about opportunities to explore ways to enhance our operations, conserve limited resources, and stimulate new ideas to more creatively execute our missions through the power of IoT and network connected sensors,” see Figure 3.<sup>[12]</sup>

A connected machine does not become “smart” from a single sensor, or modem, or network, or application alone. It is a combination of all of these pieces coming together that creates added intelligence. Smart bases are essentially the integration of networks with IoT components and data analytics to present users with situational intelligence or a common operating picture.



Figure 3. The power of IoT and connected sensors.

Why is the smart-base concept important to the U.S. Department of Defense (DoD)? Installing and integrating network-connected sensors into the everyday operations of a military installation will drive efficiencies, feed and automate analytics, bolster anti-terrorism and force protection measures, and improve processes. Typical base-level shortfalls that smart bases may remedy are increased safety and security, lower operating costs, resiliency, and infrastructure and energy efficiencies.<sup>[13,14,15]</sup> While these can be massive benefits for each functional community (finance, logistics, operations, etc.), greater and less-often discussed non-tangible benefits are increased mission assurance and mission command through enhanced, holistic sense-making, and situational awareness.

However, legacy bases today are for the most part not “smart-enabled” because they are not optimized for IoT and data analytics and this causes inefficiencies. Moreover, bases are frequently stifled by lack of manpower and budgetary constraints as well.

### ***Call to Action***

The job of securing the nation, although noble, is dirty; the operation of military facilities continues to consume enormous quantities of energy and fresh water and generates considerable amounts of waste.<sup>[16]</sup> Until recently, military infrastructures and services have been developed, operated, maintained and funded separately in their cylinders of excellence. This silo architecture has impeded the horizontal linking necessary to bring efficiencies, mission assurance, and military command. Consequently, as organizations inevitably move into the brave new world of the IoT to address these challenges, it may be easy to feel overwhelmed by the scope and complexity of the fast-materializing IoT era. Individuals and organizations can begin to reduce this complexity by understanding

the solution domain they are operating in, the target application they are addressing, and the potential solutions available within the IoT ecosystem, as shown in Table 1. These are the types of possible IoT solutions every commander should ask his or her team about when implementing smart-base solutions.

SOLUTION DOMAIN	TARGET APPLICATIONS	POTENTIAL SOLUTIONS
<b>Energy &amp; Utilities</b>	Smart Lighting Smart Metering Sensor Automation Water/Waste Management	<ul style="list-style-type: none"> <li>♦ Wireless Transport</li> <li>♦ LED Lighting</li> <li>♦ Smart Meters</li> <li>♦ Water/Gas Leak Detection</li> <li>♦ Advanced Metering Infrastructure</li> </ul>
<b>Transportation</b>	Traffic Management Vehicle Fleet Management Smart Parking Base Transit Supply Chain	<ul style="list-style-type: none"> <li>♦ Wireless Transport</li> <li>♦ Traffic Sensors</li> <li>♦ Real Time Parking Info Available to Base</li> <li>♦ RFID Tagging</li> </ul>
<b>Military Personnel Engagement</b>	DoD & Public Wi-Fi Base/Post Info Apps e-Governance	<ul style="list-style-type: none"> <li>♦ DoD, Public Wi-Fi Hotspots</li> <li>♦ Base Apps for Reporting Issues, Searching Policies</li> </ul>
<b>Infrastructure</b>	Smart Facilities Base/Post Services	<ul style="list-style-type: none"> <li>♦ Wireless Transport</li> <li>♦ Buildings, Structural Sensors</li> </ul>
<b>Safety &amp; Security</b>	Surveillance Communications Cybersecurity Hospital Capacity Tracking Fire/Noise Detection Emergency Management	<ul style="list-style-type: none"> <li>♦ Wireless Transport</li> <li>♦ Video Cameras</li> <li>♦ Intrusion Detection Sensors</li> <li>♦ Threat Intelligence Sensors</li> <li>♦ Tele-Health</li> <li>♦ Wearable Devices</li> </ul>

Table 1. IoT Solution Domains

The IoT and smart-base era is just beginning, and many aspects of securing it remains a work in progress. Organizations in every industry are already reaping the benefits of IoT implementations. By approaching the IoT strategically, and with security at the core of every connected device, military installations can begin to capture new value through the smart-base concept—while keeping potential risks in check.

Furthermore, using the DoD Mission Assurance Strategy (May 2012) pillars as a guide, strategically approach IoT implementation by using pillar one (Identify and Prioritize Critical Missions, Functions, and Supporting Assets) to guide IoT funding priorities and then utilize the IoT data and information to enable pillar three (Use Risk-Informed Decision Making to Optimize Risk Management Solutions).

While implementation of intelligent-edge devices enabling a smart-base construct may seem overwhelming, man has forever pushed himself to the limits trying to achieve the impossible. Daedalus and Icarus were imprisoned together in the Labyrinth on the Isle of Crete; they escaped on wings fashioned by Daedalus from feathers and wax. But Icarus flew too close to the sun, melting his wings, and he fell to his death in the Aegean Sea as his father sagely flew to freedom. Myth though it may be, the story of Daedalus and Icarus illustrates “the power of man has no limits” but also that this power should be employed very carefully. By weaving smart technologies at the edge into our military bases, smart decisions may be made, enabling enhanced mission assurance and military command. 🛡️

## NOTES

1. N. Bach, *Bill Gates Just Put Millions Into Building a Smart City in the Desert*, retrieved from <http://fortune.com/2017/11/13/bill-gates-arizona-smart-city-cascade-belmont/>, November 13, 2017.
2. M. McFarland, *Bill Gates invests \$80 million to build Arizona smart city*, retrieved from <http://money.cnn.com/2017/11/13/technology/future/bill-gates-smart-city-arizona/index.html>, November 13, 2017.
3. K. Briodagh, *AT&T Invests Billions to Enhance Smart City Networks in Georgia*, retrieved from <http://www.iotevolutionworld.com/iot/articles/435210-att-invests-billions-enhance-smart-city-networks-georgia.htm>, October 27, 2017.
4. K. Ashton, *That ‘Internet of Things’ Thing*. *RFID Journal*, retrieved from <http://www.rfidjournal.com/articles/view?4986>, June 22, 2009.
5. AT&T Chief Data Office, *AT&T Presentation—How Data, Analytics and Automation are Powering AT&T*, October 30, 2017.
6. A. Gabbai, *Kevin Ashton Describes ‘the Internet of Things,’* retrieved from <https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/>, January 2015.
7. International Electrotechnical Commission (IEC), *IEC White Paper—Edge intelligence*, retrieved from [http://www.iec.ch/whitepaper/pdf/IEC\\_WP\\_Edge\\_Intelligence.pdf](http://www.iec.ch/whitepaper/pdf/IEC_WP_Edge_Intelligence.pdf), 2017.
8. IEC, *IEC Orchestrating infrastructure for sustainable Smart Cities*, retrieved from <http://www.iec.ch/whitepaper/pdf/iecWP-smartcities-LR-en.pdf>, November 1, 2017.
9. Machina Research, *Machina Research White Paper—Global M2M Market to Grow to 27 Billion Devices, Generating USD 1.6 Trillion Revenue in 2024*, retrieved from <https://machinaresearch.com/news/global-m2m-market-to-grow-to-27-billion-devices-generating-usd16-trillion-revenue-in-2024/>, June 24, 2017.
10. American Society of Civil Engineers (ASCE), *ASCE 2017 Infrastructure Report Card*, retrieved from (<https://www.infrastructurereportcard.org/wp-content/uploads/2017/10/Full-2017-Report-Card-FINAL.pdf>), 2017.
11. IEC, *IEC White Paper—Smart Cities: 2014*, retrieved from <https://webstore.iec.ch/publication/22378#additionalinfo>, November 1, 2017.
12. AT&T, *AT&T and Maxwell Air Force Base Pilot IoT Connected “Smart Base,”* retrieved from [http://about.att.com/story/maxwell\\_air\\_force\\_base\\_pilot\\_iot\\_connected\\_smart\\_base.html](http://about.att.com/story/maxwell_air_force_base_pilot_iot_connected_smart_base.html), April 4, 2017.
13. T. Johnson, *Smart City Tech Would Make Military Bases Safer*, retrieved from <https://www.wired.com/2017/02/smart-city-tech-make-military-bases-safer/>, February 19, 2017.
14. Deloitte, *Smart military bases: Now is the time*, retrieved from <https://www2.deloitte.com/us/en/pages/public-sector/articles/byting-the-bullet-smart-military-bases.html#>, 2017.
15. Cisco, *White Paper: Smart and Connect Bases*, retrieved from [https://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/gov/airforce-ioe-whitepaper.pdf](https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/airforce-ioe-whitepaper.pdf), 2015.
16. NATO Science for Peace and Security Services – C: Environmental Security, *Sustainable Cities and Military Installations*, retrieved from <http://www.springer.com/us/book/9789400771604>, 2014.

# Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns\*

---

Dr. Cathy Downes

## INTRODUCTION

In January 2017, the U.S. Office of the Director of National Intelligence published a highly unusual public report outlining the Russian state-sponsored cyber-enabled campaign to distract, disrupt, and skew the 2016 U.S. elections.<sup>[1]</sup> This latest influence campaign and continuing activities in both the U.S. and other Western countries are increasingly acknowledged as part of a broader, ambitious Russian strategy of strategic competition to restore its European sphere of influence, and erode other countries' subscription to the Western liberal economic and political order.<sup>[2]</sup>

There is a growing body of evidence<sup>[3]</sup> showing Russian strategists and agents aggressively employing and leveraging an eclectic mix of interventions, including cyber/physical world creation, sharing and exploiting of disinformation and private information through social media platforms, hacking, honeypots, harassment, social botnets, astroturfing, undermining of mainstream and social media sources and content, invasive espionage, theft and exposure applications and platforms. They have also created, cultivated and exploited "useful idiots", "fellow travelers" and "agent provocateurs" as well as cyber troops, trolls and trouble-makers to borrow from the Oxford Internet Institute's Computational Propaganda Research Project.<sup>[4]</sup> Also as Pomerantsev and Weiss observe: "Feeling itself relatively weak, the Kremlin has systematically learnt to use the principles of liberal democracies against them in what we call... "the weaponization of information, culture and money," vital parts of the Kremlin's concept of "non-linear" war."<sup>[5]</sup>

There is growing understanding of *what* has been done in the Russian campaign. Rather less consideration has been given to *why* the campaign has been able to achieve the effects evidenced. Certainly, some credit must go to the innovativeness of the

*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. Cathy Downes has been a Professor of the National Defense University's College of Information and Cyberspace since 2003. She holds Ph.D. in International Relations and Strategic Studies from the University of Lancaster, United Kingdom. She is also an Australian Defense Industrial Mobilization Course graduate and holds a U.S. Department of Defense Chief Information Officer Certificate. Dr. Downes has held research fellowships at Harvard University's Center for International Affairs, University of Melbourne and Australian National University before serving as a senior civilian executive in the New Zealand Defense Force, leading enterprise transformation initiatives and as a defense policy writer and adviser. She leads the College's Cyber Leadership and JPME II program courses on National Security and Cyber Power Strategies and Multi-Agency Collaboration. Her research interests include: concepts of international cyber power, strategic thinking and national security strategy formulation, an inter-agency collaborative maturity model, technology futures assessments, and digitally-enabled learning environments.

Russians. Their "active measures" have evolved to leverage new capacities and target vulnerabilities created by the unique features and dynamics of cyberspace and Western populaces and their polities.

But it is also the case that the campaign's successes are partially due to miscalculation, and mistakes—strategic blind-spots—on the part of Western national security policy leaders and practitioners. These have created opportunities and weaknesses that Russian disinformation tactics have been able to capitalize on.

A "blind-spot" is an area of the eye's retina that is "insensitive to light." More colloquially, it is an inability to understand something or see how important it is. More pointedly, a blind-spot is a prejudice or area of ignorance that one has but is often unaware of.<sup>[6]</sup> Blind-spots cause or contribute to reasoning and decision failures—(1) not "connecting the dots" about causes and effects in time to take necessary action; (2) not imagining real possibilities and reacting accordingly, and (3) not taking corrective action. For national security policy leaders and professionals, strategic blind-spots create opportunities for being surprised by what they have not had the situational awareness to anticipate. Further, if a person or group is unaware of a blind-spot, and consequently does not address this defect, the likelihood of poor reasoning and decisions is substantively increased.

In the case of the Russian influence campaign leading up to and beyond the 2016 US elections, a number of strategic blind-spots can be highlighted. Recognizing and addressing these is critical to the design of effective deterrent and response national security strategies. Assumptions need to be challenged; cognitive biases recognized and corrected, and perspectives broadened. Sans these self-assessments, any strategic calculus to frame

countermeasure strategies are likely to be insufficient or flawed, allowing conditions to persist that will aid future Russian and copy-cat cyber-enabled threats, vectors, and campaigns.

### ***Overlooking a Critical Target and Underestimating Threats to it***

The Y2K experience revealed the extent of dependence upon computer systems in highly industrialized societies and economies. Since then, this reliance has only increased and spread to every industry and government sector. The “surface area” to be secured continues to expand exponentially with developments such as IPv6, social media platforms, the Internet of Things, and global growth in Internet/mobile devices and users.

At the same time, the commercial first-to-market competitive pressures have often proven greater than warnings of the need for the early design of security features in products. As a consequence, the roll-outs of hardware and software have included bugs, flaws, and other vulnerabilities. These have been matched by the growth of an “alt” industry for building and distributing hacks and exploits that take advantage of or address these vulnerabilities.

As a result, governments and businesses have fixated on defending and protecting their data, IT devices, systems, and networks from pernicious penetration and exploitation attempts and successes by state-sponsored and non-state cyber thieves, spies, hacktivists, and hoodlums. As one industry analyst observed: “IT analyst forecasts are unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyber-attacks launching at businesses, governments, educational institutions, and consumers globally.”<sup>[7]</sup> The string of recent high profile cyber breaches and thefts have placed increasing pressures on governments and businesses to double-down on investing in cyber defenses. Dramatic estimates of the costs of these breaches, the costs of cybersecurity and workforce-related requirements reinforce the focus.<sup>[8]</sup>

In 2013, the Obama Administration issued Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, which replaced the 2003 Homeland Security Presidential Directive 7 on the same subject. PPD-21 aimed at “...taking proactive steps to manage risk and strengthen the security and resilience of the Nation’s critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health, and safety or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats and hasten response and recovery efforts related to critical infrastructure.” The Directive

\* The views expressed are those of the author. They do not necessarily reflect the policies of the U.S. Department of Defense, National Defense University or the College of Information and Cyberspace. The author wishes to thank Dr. Paul Shapiro and NDU CIC faculty for helping me clarify my thinking on a key aspect of this article.

identified 16 “Critical Infrastructure Sectors” and matched each to a “Sector Specific Federal Agency or Department” under the overall coordination of the Department of Homeland Security.<sup>[9]</sup> The only sector of relevance to governing the nation was that of “Government facilities” being concerned primarily with protecting government buildings and national monuments and icons.<sup>[10]</sup>

Unfortunately, the concept of “infrastructure” was limited to physical structures, and technical control systems and assets. Inevitably, this approach channeled thinking and assessments of the types of threats that can, and are, threatening these targets, particularly regarding terrorism and cyber assaults. Within PPD-21 there are 16 critical infrastructures are drawn from those identified in the U.S.A. Patriot Act 2001 that defines criticality as being “so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety...” Most dictionary definitions of infrastructures also include the qualifier of being “needed for the operation of a society or enterprise.”<sup>[11]</sup>

When these perspectives are brought into a concept of critical infrastructure, it would seem that one infrastructure needed for the operation of a society was overlooked the US system of political governance; encapsulating a political system for choosing and replacing governments through free and fair elections whose results are accepted societally; active participation of citizens in politics and civic life; protection of human rights, and equality under the law.<sup>[12]</sup> Nested in this system are politicians, candidates for political office, political parties, campaigns, donors and staffs, constitutional provisions for elections, and most particularly the views, perspectives, beliefs, and understandings of eligible and future voters.

Yet, even when it became apparent by mid-2016 and through early 2017 that the Russians had engaged in a concerted information campaign against the 2016 elections, US government responses were dominated by technical thinking. This was demonstrated in the January 2017, decision to only modify the Government Facilities Critical Infrastructure Sector to include “the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.”<sup>[13]</sup>

The issue of foreign interference in the 2016 election had become a hot topic of discussion in 2017. Yet, within this, little concern seems to have been raised over the absurdity and inadequacy of taking actions to secure voting machines, *after* agents of a foreign power acted to subvert and manipulate the cognitive decision choices of voters before they even arrived at the polls. Lacking tools to show irrefutable evidence of impact, it would seem that it was merely assumed that foreign interference would have no impact on the minds and choices of voters. However, as further evidence of the extent and creativeness of the Russian influence campaign emerges, the grounds for this assumption are becoming more questionable.

Diverted by the obvious urgency to secure technical systems, national security policy-makers and professionals failed to recognize the “weaponizing” of internet content as a threat, the US political system as an infrastructure of criticality for the effective functioning and security of the US government and society, and the voting public, as the target. In testimony before the U.S. Senate Armed Services Subcommittee on Cybersecurity, in April 2017 Rand Waltzman remarked: “Today...the manipulation of our perception of the world is taking place on previously unimaginable scales of time space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities ...Information environment security today is primarily concerned with purely technical features...This view is too narrow.”<sup>[14]</sup>

### ***Strategy and Strategic Thinking Required as Much as Military Doctrine***

The Royal United Services Institute (RUSI) Director of Military Sciences Peter Roberts observes that “...the West’s understanding of war remains essentially Napoleonic: organized campaigns, orchestrated by a central staff...[but] the enemies of the West have reconstructed conflict and reimagined warfare to suit their own ends. Against this, the West has failed to appreciate...that way of considering the world, and remains bound by the codification of warfare put forward by Clausewitz, J.F.C. Fuller and Basil Liddell Hart...the Western focus is on the way adversaries act at the tactical level, not on understanding the nature of change that has occurred in their way of fighting. A belief in Western conceptual or intellectual superiority remains deeply entrenched in the Western orthodoxy; such hubris has distinct dangers.”<sup>[15]</sup>

Evidence of Russia’s influence and manipulation campaign supports Dr. Robert’s tough and discomfoting assessment that highlights a second blind-spot of US national security policymakers and practitioners. This concerns the dominant influence of military doctrine thinking and concepts upon US grand and national security strategy and strategic discourse.

Military doctrine serves to codify best military practices from primarily historical experiences. It is also used to translate...the higher conceptualization of war...into working guidelines for action.”<sup>[16]</sup> There are risks in this power as British military historian Sir Michael Howard warns that: “...the soldier has to steer between the dangers of repeating the errors of the past because he is ignorant that they have been made, and of remaining bound by theories deduced from history although changes in conditions have rendered these theories obsolete.”<sup>[17]</sup>

The evolution of US military and joint doctrine over recent years has had some relevant unintended consequences. For example, Kelly and Brennan in their 2009 U.S. Army War College Strategic Studies Institute monograph, *Alien: How Operational Art Devoured*

*Strategy* examine how the US doctrinal focus on the operational level of war, and operational art has in many ways supplanted strategic conceptualizations and consigned political and policy leaders to the role of “strategic sponsors.”<sup>[18]</sup>

Over the last decade particularly, Russian civil and military leadership have evolved a broad and multi-faceted grand strategy for strategic competition with the Western liberal economic and political order. By contrast, US military doctrine, perspectives, mindsets, and priorities have become the significant dynamic in the meager space of Western and US strategic thinking and discourse devoted to the impact of cyberspace on international security relations, strategy and the strategic application of the information instrument of national power. Kelly and Brennan observe: “[operational art] has come to compete with strategy rather than being its humble servant.” They question whether recent Western military failures are the result of endemic weaknesses or possibly due to: “...allowing operational art to escape from any reasonable delimitation and, by so doing, subvert the role of strategy and hide the need for a strategic art?”<sup>[19]</sup>

As discussed above, military understandings of cyberspace, cyber power, and strategy options that particularly leverage both, have been preoccupied with tactical and technical responses to threats to U.S. Department of Defense (DoD) computer networks and systems. As the strategic theorist, Colin S. Gray observes: “High-quality strategic theory about cyber simply is not there in the literature...The negative comparison with the nuclear debate in the 1950s is almost extraordinary in its scale and quality.” He goes on to observe that: “...to risk understatement, most of this literature, though no doubt valuable in its own right, has been innocent of, or naïve about, strategic considerations.”<sup>[20]</sup>

This is not to deny the significance of such threats or the vulnerability for US military forces whose technology development path over the last decades has focused on sustaining a conventional battlefield “speed of thought and adaption” edge through the advantages of enhanced situational awareness and self-organization enabled by networked information systems. In response, priority has been placed designing, resourcing and executing “cyberspace operations” to protect DoD and military missions in and through cyberspace.<sup>[21]</sup> The case for priority and attention has been intensified by high profile cyber thefts and evidence of mass attempts at network penetration.

Over the same period, comparatively, the significance and resources assigned to US military “information operations”<sup>[22]</sup> has faded. In the US, the case for such operations has been influenced by “...a peculiarly American outlook that using persuasion and influence at the national level is somehow unethical and inconsistent with a democracy, that using “psychological tricks” is “dirty” and immoral, and that it’s completely unnecessary... the United States should just factually show the world who we are, and everyone will automatically recognize how wonderful we are and want to emulate us. The successful propaganda efforts of US enemies also contributed to the American distaste in many circles... Anything that smacked of propaganda or psychological warfare became something that only the “bad guys” did.”<sup>[23]</sup>

Despite the energy of IO advocates, wide-scale and insightful understanding of changes in the information environment have been slow to gain traction in the US military doctrine and national security communities. The viral emergence of the interactive web, the blogosphere, the exponential growth and uses of social media platforms have tended to be restricted to a military context and sadly often limited to a narrow concern over whether troops and employees are being distracted from their work by “socializing on Facebook.”

Doctrinally and legally, such operations have been treated only within the context of US military operations in overseas theatres and to support U.S. Combatant Commanders.<sup>[24]</sup> By contrast, the growing body of evidence of Russia’s on-going “active measures” campaigns in Europe and the US shows that Russian civil and military leaders have elevated information operations to a full-blown instrument of strategic influence, both “narrative power”<sup>[25]</sup> and disruptive power, mainly taking advantage of national border-agnostic developments and capabilities of the interactive social Internet.

There has been an increasing divergence between Western and particularly US conceptions and approaches to strategic competition, conflict, war and military operations, and those of the national security communities of countries such as Russia and China. This is again well summed by RUSI Director of Military Science Roberts: “...the West’s enemies see the battlespace as a whole, a global environment not confined by the limits the West has imposed on it...individual domains, areas, theatres and concepts are all linked and are intrinsically part of the contest. Boundaries do not exist for them, and where the West constructs them, they see weaknesses and vulnerabilities to exploit. They intrinsically use confusion, distraction, deception and obscurity to achieve long-term goals, accepting that failures and losses are part of that journey.”<sup>[26]</sup>

Particularly post-September 11, 2001 attacks, with with a partial exception of the Obama Administration, US national security leaders have relied more intently upon the military instrument in national security strategy and statecraft. The US has doubled-down on its hard power capacities. In response, other lesser military powers have increased their leveraging particularly of the informational instrument’s soft power advantages while continuing to upgrade their military capabilities organically and those for cyber espionage.

Moreover, in the most recent period, changes in US international policies have undermined many sources of national soft power.<sup>[27]</sup> This is somewhat ironic at a time when other national leaders have perceived the significance of leveraging soft power through, and in, cyberspace as one of the critical changes in nature of international strategic competition, and acted upon that perception, as Director of the European Council on Foreign Relations, Mark Leonard remarks: “The most important battleground of this conflict will not be the air or ground but rather the interconnected infrastructure of the global economy: disrupting and controlling trade, investments, currencies, international law, the internet, transport links, and the movement of people, employing boycotts, sanctions, disinformation, Welcome to the connectivity wars.”<sup>[28]</sup>



Following his analysis of the Arab Spring, it is interesting to note the Russian Chief of the General Staff's 2013 reflections on how the Western way of war had evolved, perceptively observing a four-to-one ratio of non-military to military measures. General Gerasimov and others in the Russian national security community have possibly read more strategic calculus and coordination in Western actions than is merited. Nonetheless, it would seem that Russian leaders have followed this ratio in designing a grand strategy of competition that leads with the information instrument of national power's 21st century disinformation and cognitive hacking interventions.

Historically, Western military doctrine has regularized novel conditions and capabilities by fitting them into accepted ways of organizing and thinking. In each case, an internecine dynamic plays out where some advocates seek to create new distinct structures, authorities, and practices while others seek to fit new conditions and capabilities into extant unit, rank structures, tactics, techniques and procedures, and culture. The press to institutionalize cyberspace (as the fifth domain) and cyber capabilities within extant US military models is evident in actions such as the standing up U.S. Cyber Command (USCYBERCOM), its 2017 elevation as a full unified combatant command, the 2015 DoD Cyber Strategy<sup>[29]</sup> and multi-million dollar resourcing of "Cyber Mission Forces" cyber "warrior career" paths, etc. with the primary emphasis on forces and capabilities for protecting and defending DoD networks and systems, and supporting the needs of U.S. Joint Force Commanders in the conduct of conventional operations.

The focus of these efforts is underpinned by an untested assumption: that the other US military services, joint organizations and operational doctrine offer the best model for organizing information and cyberspace national security capabilities. Yet, if we take as a small point of comparison: while the US has focused its investment on developing regularized military professional Cyber Mission Forces, the Russian Federation has invested in, sponsored and leveraged an eclectic lineup of irregular, civilian hackers, ad click-bait entrepreneurs, proxy non-governmental organizations, automated computer algorithm botnets, "useful idiots" within the US and other Western countries, and a low-cost, deniable, easily-expandable "troll army" of social media commentators and post authors.<sup>[30]</sup>

This comparison is not to recommend that the US match Russian troll armies. It is to suggest that a purely military model of capabilities and structures for responding to information and manipulation campaigns may not necessarily be optimal.

Legitimizing novel conditions and capabilities by incorporating them into proven and prescriptive operational military doctrine models is also pre-empting intellectual efforts to assess and explore the impact of cyberspace upon international security relations. As a consequence, we have seen the comparatively uncritical transference of concepts of international security relations that have evolved within and respond to a quite particular and different strategic context. A classic example of this is the US defense community-

sponsored push to formulate concepts of cyber deterrence. As MIT's Nazli Choucri's points out: "When we compare these unique and defining characteristics of cyberspace, it is evident that the major trajectories, dynamics and consistencies of international relations, established particularly throughout most of the 20th century cannot be readily or uncritically imported into international relations in and through cyberspace in the 21st century."<sup>[31]</sup>

This raises the more significant question as to whether the conditions and dynamics of cyberspace require an *a priori* period of similar critical examination to that given by international relations scholars, thinkers, and strategists during the 1950s and 1960s about strategizing to cope with the advent and proliferation of nuclear weapons. One of those scholars, Professor Brodie, in *Strategy in the Missile Age* (1959) observed: "There is an intellectual no-man's land where military and political problems meet. We have no tradition of systematic study in this area, and thus few intensively prepared experts. The military profession has traditionally depreciated the importance of strategy (where politics are important) as compared with tactics. Now we are faced with novel and baffling problems to which we try to adapt certain ready-made strategy ideas inherited from the past."<sup>[32]</sup>

While the destructive capacity of nuclear weapons is proven unequivocally and the possible destructive effects in cyberspace are not, arguably we are in a similar intellectual no-man's land. Cyberspace, and its demonstrated and evolving potential uses for strategic effect, do not fit neatly into existing operational and strategic concepts. Instead of borrowing and shoe-horning existing strategic and international relations concepts, there is a need to devote strategic thought into formulating more original strategy and foreign policy ideas and approaches that can appropriately guide military doctrine thinking and development.

Finally, in many respects, it would seem that the US national security establishment has fallen foul of the national security blind-spot equivalent of Harvard University's Professor Clayton Christensen's Innovator's Dilemma.<sup>[33]</sup> As noted above, unable to compete directly with the U.S. military power advantage, countries, such as Russia and China, have evolved strategies favoring less expensive, more adaptive non-military instruments of national power, while continuing to build up their military capabilities. As with Christensen's model for businesses, the US has focused on ever expanding the over-match of its military power capabilities to counter the military capabilities of competitors.<sup>[34]</sup>

In Christensen's business model, new entrants with few resources innovate with technologies and markets, producing goods and services viewed by mainstream businesses as cheap, tacky, and lacking in features attractive to their customers. As a consequence, new entrants are not viewed as threats. Failure comes when the upstart advances rapidly entering the more mature markets of incumbents and disrupting them.<sup>[35]</sup> While certainly not new entrants, re-emergent and revanchist powers, such as China and Russia, are playing the new entrant role.



Thus, while the US defense community and industrial base has been preoccupied with over-matching the military capabilities of competitors, the Russians have applied an out-flanking strategy-level “offset” of a different sort. As Paul and Matthews: “Russia has taken advantage of technology and available media in ways that would have been inconceivable during the Cold War...Experimental research in psychology suggests that the features of the contemporary Russian propaganda model have the potential to be highly effective.”<sup>[36]</sup>

In concentrating on cyber threat vectors for obvious data and information theft, malware, denial of service assaults to the technical layers of cyber infrastructure, and on over-matching conventional and strategic military capabilities, national security policy makers and practitioners have overlooked the larger cyber-based threats to the US political system that have been created. Klimberg observes: “through a subtle reframing of information overall as a weapon...we have moved toward a reconceptualization of interstate conflict and “war” altogether, one where states routinely engage in hostile acts that skirt around and under the threshold of recognized war and increasingly manage to reposition “information” including everything from computer viruses to the workings of the media, as a weapon, with potentially existential implications for democratic societies.”<sup>[37]</sup>

### ***Strategic Center of Gravity or Critical Vulnerability or Both?***

All US National Security Strategies declare: “The United States government has no greater responsibility than protecting the American people.”<sup>[38]</sup> Yet, both national and subordinate strategy documents, such as the national military strategy, narrowly focus only on conventional threats of kinetic violence employing land, maritime and/or air-deployed weapons and tactics, or the unconventional threats of violent extremist groups.

This assessment leaves unconsidered threats that do not depend on destruction of life and property to achieve desired outcomes, including “...the use of information and communication technologies, services, and tools to create and spread stories intended to subvert and undermine an adversary’s institutions, identity, and civilization, and it operates by sowing and exacerbating complexity, confusion, and political and social schisms.”<sup>[39]</sup>

Any robust threat assessment focuses on two factors—the threat’s intentions and capability, and the strengths and defenses of that which is threatened. Yet, the US national security community has underestimated the threat posed by Russia’s grand strategy and influence campaign. It has also underrated, if not assiduously avoided assessing, the vulnerabilities of the US populace and polity, and Western partners and allies, to being targeted by this campaign. Overlooking these vulnerabilities substantially weakens any strategic calculus for effectively countering such tactics.

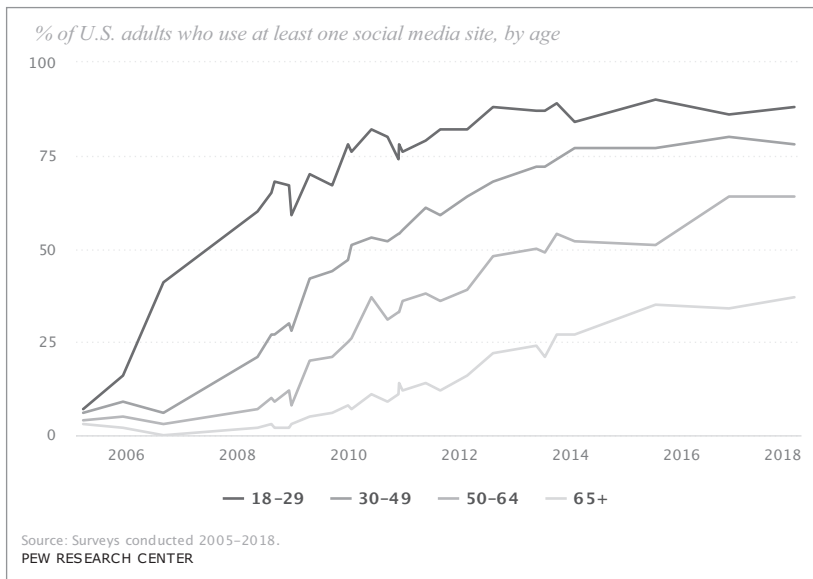
An examination of conditions and circumstances shows the US population and its political system as a particularly soft target, as Brad Allenby observes: “...a number of

trends are coming together to create a unique historical period, one in which weaponized narrative not only has a privileged position as a weapon of choice to use against otherwise conventionally well-armed adversaries, but in which the United States is uniquely vulnerable.”<sup>[40]</sup>

Dependent upon free-and-fair citizen elections to legitimize changes of government, representative democracies provide scheduled and frequent targets for disinformation campaigns. This dependence and the opportunity it provides is not new. What has changed is the vulnerability of voters to manipulation that leverages their increasingly rich and predictive digital foot-prints. Data and information about voters preferences and predispositions is increasingly for collection and sale through new enabling applications for online and offline shopping, internet search data on habits, financial transactions, online news viewing, commenting and sharing, cell phone usage, blogging, virtual worlds, social and video communications via online media platforms, the Internet of Things and data from surveillance devices. While primarily generated for commercial marketing purposes, the populace’s Internet engagement has provided an exponentially expanding equal-opportunity source of data for political campaigns *and* foreign disinformation campaigns.

Such databases can significantly empower political campaigns and candidates to engage and inform potential voters cost-efficiently. At the same time, the data trails left by voters provides campaigns with the increasing ability to psychometrically profile, compose and target messages to individual voters that intensify and amplify, rather than reduce, their cognitive biases and preconceptions; that can disinform as much as inform. Evidence continues to build of such leveraging of voter data in the US 2016 election being used to manipulate voter choices about their intentions about voting and how to vote raising the possibility of indirect suppression and invalidation of votes. Notable example of these tactics included the data and predictive analytics and ad micro-targeting employed by UK Company, Cambridge Analytica, and the use of targeted deceitful and misleading content messages through the Facebook and Twitter platforms such as the fraudulent vote-by-text message.<sup>[41]</sup>

The US population is particularly vulnerable to such targeting because of its high reliance on cyber interconnectivity, sourcing of news and social/political engagement. For example, in 2016, the global average internet penetration was 50%; for the United States, it was 88%. For social media penetration, the global average was 37%; for the U.S. it was 66%. In comparison to the 55% global average, 70% of US Facebook users use the platform daily.<sup>[42]</sup> In Pew Research Center surveys, in 2005, just 7% of American adults used social networking sites. By 2017, 69% of American adults used such sites and of those Americans using Facebook, just under half (45%) get their news from Facebook, and 26% of all US adults get news from two or more social media sites.<sup>[43]</sup>



<http://www.pewinternet.org/fact-sheet/social-media/>

Appearing before the U.S. Senate Select Committee on Intelligence in late 2017, Facebook’s Legal Counsel, Mr. Stretch testified that Facebook had identified “... a total of 80,000 posts and ads from Russian-backed accounts [from one source—the Russian Internet Research Agency] were seen by 126 million people through flow-on effects of interconnected users, uncritically sharing with other users in their personal networks over a period of two years.” Twitter and Google Legal Counsels also presented estimates of Russian activities on Twitter and YouTube.<sup>[44]</sup> These numbers were down-played disingenuously referencing the larger scale of total activity on these platforms. However, it would seem that Russian-backed disinformation posts and ads reached over 50% of Facebook’s US users. Moreover, no assurance was given that the full scope of Russian disinformation activities had been discovered.<sup>[45]</sup> Further, these figures do not reflect the additional effects of data analytic companies leveraging data on users’ sharing and “likes” to tailor ad buys to disseminate intentionally or unintentionally similar sentiments and messages to those of Russian engineered content.

The degree of connectivity is also reflected in the broader Facebook “universe” of ways in which people (and computer-algorithm social bots acting as people) can share disinformation and their own personally identifiable data as much as information. These include Facebook-owned social media messenger and chat apps—Facebook Messenger, WhatsApp and Instagram with duplication through easy-use cross-posting between these apps. These all increase the scale and density of virtual tributaries and arteries that can be penetrated and leveraged by disinformation campaigns not only by Russia but also by a variety of existing and future non-state actors.

Significant upgrades in mobile devices, interactive web and blog apps, livestreaming capacities, and monetarization models have all reduced entry barriers—or “democratized”—the human and botnet creation and wide-scale distribution of all types of “news” content, including an increasing array of user-produced video.<sup>[46]</sup> This has substantially expanded the scope and availability of unfiltered, un-aggregated, and un-mediated content that Americans are exposed to through their Facebook accounts and in the broader Internet. This content access is also influenced by online news aggregator and filter bubble apps that tailor and shape what users view, read or interact with.<sup>[47]</sup>

Further, earlier Soviet-era influence campaigns had the goal of weaving a strategic narrative of a positive image of the communist political and economic system. By contrast, the contemporary Russian campaign in the US 2016 elections, for example, appear to have shifted to a more achievable and less challenging goal; that of promoting distraction, confusion, doubt and mistrust, with almost an equal-opportunity approach to targeting disinformation, emotionally charged histrionic news items and comments on all sides of the political spectrum. For example, in looking at Russian “information warfare,” Keir Giles observes: “...Unlike in Soviet times, disinformation from Moscow...has as one aim undermining the notion of objective truth and reporting being possible at all...the new vulnerability that current Russian campaigning can exploit is, in the words of veteran scholar of Russia Leon Aron, Western societies’ “weakened moral immunity to propaganda” and “weakness of confidence in sources of knowledge.”<sup>[48]</sup>

As a consequence of the density and diversity of connectivity and the proliferation of content, voters are increasingly overwhelmed and under-equipped to distinguish fact from fiction. Distinguishing whether any, all or some content is truthful, useful, or customized disinformation inserted by foreign state agents or non-state actors or legitimate political campaigns is increasingly challenging. Moreover, as online advertising have successfully drawn off ad revenues from “mainstream” media organizations, such organizations, even in their online formats, have had fewer resources to serve as filters for objectivity and accuracy.<sup>[49]</sup> Furthermore, responses to information overload also can have particular counter-intuitive effects that are not necessarily recognized by voters. For example, Paul and Matthews in examining the Russian propaganda model note that: “When information volume is low, recipients tend to favor experts, but when information volume is high recipients tend to favor information from other users...The experimental psychology literature suggest that all other things being equal, messages received in greater volume and from more sources will be more persuasive. Quantity does indeed have a quality all of its own.”<sup>[50]</sup>

Exposed to overwhelming amounts of information, steered by filters and news aggregators, and targeted by their cognitive biases and digital footprints, it is not surprising that a portion of the electorate has been deceived by content that caused confusion, distraction,

distrust or a retreat into an echo chamber that reinforced their preferences. This too has served both the goals of legitimate political campaigns and foreign influence campaigns, as once deceived, it is extremely difficult for anyone to admit that they have been gulled, and the evidence threshold for such an admission is commensurately heightened.<sup>[51]</sup>

The health of political discourse itself makes the US population and polity particularly vulnerable to cyber-enabled disinformation campaigns. Such campaigns delight in high levels of political discord and discontent. There are always going to be differences of opinion on any issue. However, partisan US political discourse has become deeply polarized in the last decades. The Pew Research Center's October 2017 survey observed that: "The divisions between Republicans and Democrats on fundamental political values—on government, race, immigration, national security, environmental protection and other areas—...have increased dramatically...And the magnitude of these differences dwarfs other divisions in society, along such lines as gender, race and ethnicity, religious observance or education."<sup>[52]</sup> The greater the degree of difference of political viewpoints and values, the greater the number and intractability of "wedge" issues, the more openings for disinformation messaging by foreign agents, indistinguishable from those of domestic political campaigns, which intensify and amplify distrust and disagreement with "the other."

At the same time, in the intensifying competition between television and online media organizations to sustain commercial viability by "...harvesting human attention and reselling it to advertisers," political discourse has become sensationalist political theatre, to entertain, not necessarily inform. Elections are political dramas. Contextualized as slap-down grudge matches, events are analyzed minutely and re-hashed by 'expert commentators' representing particular polarized viewpoints and opinions. The almost oxymoronic continuous "Breaking News," "Countdown" clocks to candidate debates which are themselves aired and streamed online as gladiatorial gotcha contests, are designed to grab and hold viewer attention. This is in addition to the efforts of political campaigns to out-do each other in both the frequency and shock/scandalize factor spin-doctored half-truth negative attack advertising on television, in robo-telephoning and distributed through web-and social media-based micro-targeted messaging.

Add into this cacophony of attention seeking sound-bites, where nothing can be denied for fear of a First Amendment Right to Free Speech challenge, the internet-leveraging "click-bait" entrepreneur.<sup>[54]</sup> Such actors purposefully eschew accurate, objective professional standards of journalism, recognizing that strongly negative or positive headlines tend to attract more viewers and therefore earn them more ad dollars.<sup>[55]</sup> Moreover, it is difficult for viewers to distinguish the motivations and origins of such actors—purely financial, foreign or domestic, political advocacy, or part of a Russian or non-state actor disinformation and manipulation campaign.

The quality of political discourse in the US 2016 election was further influenced by a significant increase in the exposure of voters to “fake news” or “distorted signals uncorrelated with the truth” mainly conveyed through social media platforms and websites designed to influence or confuse voters contextual understanding and candidate/party choice. Allcott and Gentzkow in their research findings on a database of just 156 false election-related news stories on social media assess that there was upwards of 760 million instances of a user clicking through and reading one of these 156 fake news stories. They note that a list of fake news websites, on which just over half of articles appear to be false, received 159 million visits during the last month of the election.<sup>[56]</sup>

Unfortunately, voters have not been helped to identify and distinguish accurate, objective, factual information from falsehoods and fabrications by the recent political practice of diversionary labeling of inconvenient or uncomfortable information as “fake.” Moreover, this practice has opened up a small industry in fact-checking sites that in turn have generated Russian government and likely government-sponsored fake fact-checking sites that label accurate information as fake.<sup>[57]</sup>

At the same time, there has been an increase over the last decade particularly in policy advocacy groups paying universities and think-tanks to secure academic credibility for their particular agendas<sup>[58]</sup> This has likely reduced the uniquely valuable contribution such institutions make to the plurality of in-depth research and analysis of critical policy issues. This robust diversity is an essential part of broadening and testing ideas and proposals in political discourse and policy debates. It is also crucial for exposing, for policymakers and practitioners, policy positions based on falsehoods, and biased analysis.<sup>[59]</sup>

### ***Opening the Aperture***

The physiological blind-spot in the human eye is where the optic nerve takes up the space of retina cells. The brain has an autonomic response that “fills in” information about what is most likely in the missing area. By contrast, the strategic blind-spots outlined above do not have a similar aid. Where they have been spied, most US national security policymakers and practitioners recognize them as wicked problems with innumerable causes; lacking a right answer; the opposite of hard but ordinary problems, which can be solved in a finite time by applying standard techniques; and where conventional processes fail, they may exacerbate situations generating undesirable and unintended consequences.<sup>[60]</sup>

Furthermore, the US national security policymaking architecture that should address these blind-spots is fragmented and fractious. It is bifurcated and bounded into externally and domestically facing sets of constitutional, administrative and legal precepts and arrangements. Like other contemporary issues (climate change, globalization, cyberspace governance), these arrangements, designed for the US political context of the late 1700s, are ill-equipped to respond to threats such as the Russian influence campaign. State



Department Public Diplomacy is legally bound to gaining foreign publics' support for US national interests.<sup>[61]</sup> The Department of Homeland Security limits its protection to how it defines Critical Infrastructure that only calls for protecting hardware and software, not human wetware. The DoD defends its computer networks. The Department of Health and Human Services and Centers for Disease Control and Protection each have their bounded area of specialist expertise and responsibility etc. for the American people. As Klimberg observes regarding cybersecurity but which applies equally well to efforts to respond to the Russian information campaign: "...each distinct aspect of cybersecurity... operates ...a specific government department or ministry. Each of these silos has its own technical realities, policy solutions and even basic philosophies...it is likely that you will not have the time to acquire more than a rudimentary knowledge of the others. Your part of the elephant will dominate and inevitably distort how you see this beast."<sup>[62]</sup> These structural divides are also mirrored in the division of law, authority and resourcing priorities at the state and local levels that challenge issues requiring national coordination and collaboration.

Thus, US governance systems struggle for systemic, whole-of-government approaches. This leaves a confusion of duplication and overlap as well as the vulnerability of seams and gaps so that little is provided to assist voters, political campaigns, and government leaders to distinguish between legitimate, First Amendment protected information and injects of disinformation by foreign agents or non-state actors. Moreover, these systemic challenges impede efforts to design and execute effective national security and cyber power strategies to address Russia's grand strategy of strategic competition with the West and the US in particular, and its use of cyberspace and information interventions to shape the security environment short of kinetic war.

Furthermore, given that effective strategy formulation requires context, there is a critical need to examine the next likely steps that the Russians may take. On the one hand, there is a natural inclination to "stick with a winning formula." Many US national security analysts and researchers are exposing the effects of the Russian information campaign during and after the 2016 US elections. Why quit doing what you are doing when it is evident that you are doing well?

On the other hand, unlike the physical air, land, sea and space domains, cyberspace and its data and information are constantly morphing and expanding as new technologies, opportunities, and risks for their use are created, as co-founder and chairman of the X-Prize Foundation Peter Diamandis remarked in February 2017: "advances in quantum computing and the rapid evolution of AI and AI Agents embedded in systems and devices in the Internet of Things will lead to hyper-stalking, influencing and shaping of voters and hyper-personalized ads, and will create new ways to misrepresent reality and perpetuate falsehoods."<sup>[63]</sup>

For example, expect new applications to manipulate video, transferring the idea of creating fake images and false text, tweets and retweets, to composing fake virtual reality/holographic projections for use in video. Political campaigns will need to prove that videos/TV presentations/commentators/leaders are real not fake. We are also likely to see advances in persuasive technologies to influence users through queuing autonomic responses to superficially innocuous messages for action.<sup>[64]</sup> Inevitably, developments in machine learning will make it almost impossible to distinguish a bot from human and human from a bot. We may need to rethink Abraham Lincoln's maxim that: "You can fool all the people some of the time and some of the people all the time, but, you cannot fool all the people all the time" as Helbing et al. remarks: "We are being remotely controlled ever more successfully...The trend goes from programming computers to programming people...a sort of digital scepter that allows one to govern the masses efficiently without having to involve citizens in democratic processes."<sup>[65]</sup>

The Russians may take a low-risk approach of doubling-down on their extant playbook of disinformation tactics and tools to replicate, if not entrench, the conditions of distraction, confusion, and distrust they have generated to date. The risk in this is that the US and Western allies will develop information intervention strategies to counter such efforts. Alternatively, they could change out the playbook with new combinations of existing and emerging data and information manipulation tools and tactics.

This prospect doubles the challenges for US and Western national security policy leaders and practitioners. There is a need to recognize and address strategic blind-spots impeding and diverting accurate threat and target identification that informs the development of effective strategies. Then, there is the need to formulate and execute strategies that can blunt and overturn current Russian information manipulation efforts *as well as* keep a countering pace in designing complementary diplomatic, informational, military and economic interventions that outflank how the Russians may choose to evolve their playbook.

Such strategies are beyond the remit of this paper. However, there are some actions that may contribute to improving the necessary conditions for sound strategy work by addressing the strategic blind-spots outlined here. Admittedly none are uncontentious or easy quick wins or low-hanging fruit. This is unrealistic when dealing with a wicked problem. The first and obvious recommendation is that policy leaders and practitioners recognize the US political system as a critical infrastructure, essential for the peaceful, stable functioning of a democratic American society, which is being threatened and targeted and requires national protection.

Policy leadership is needed to prioritize and resource at least five major research and development initiatives. The first concerns engaging with the broader national and international security relations and advanced technologies academic community in a concerted research initiative on the international security relations of cyberspace and cyber power.




The aim of this initiative would be to adapt existing concepts of international security relations and formulate original concepts of cyber power to better guide diplomatic and military interventions.

The second concerns a concerted research effort on emerging bio-robotic-info-nano technologies that could create new tactics and tools for both disinformation and for transparency. There is a need to examine the opportunities for foreign state actors, but equally copy-cat or original campaigns by non-state actors. Such an initiative should engage policy advisers, practitioners, industrialists, academics, and non-traditional participants. In a similar way to leveraging Hollywood screenwriters and directors who were reportedly asked by the U.S. Army to think up terrorist scenarios after the September 11 attacks, this research effort should engage diverse contributors from psychology, history, sociology, international security relations, political and behavioral sciences, advertising, marketing and strategy backgrounds.

The third concerted research effort needs to be led by the tech industry to design applications, protocols, machine learning features, rating systems, that *a priori* alert users to false/misleading information and disinformation before they interact with it. After-the-fact, fact-checkers are a whack-a-mole non-solution. Similar in concept to Secure Socket Layer Certificates for example and other applications that identify high-risk sites, and allow users to configure their settings to filter them out, the aim would be to tag disinformation sites and their content with the cyber equivalent of radioactive tracers or labels.

The fourth concerted research effort needs a “top-minds” legal taskforce to examine the weaknesses and vulnerabilities of US laws regarding regulations on political campaign advertising, “hate speech,” privacy and control over personal data and information, etc. While any regulatory effort is likely to conflict with the First Amendment, this does not detract from the necessity of such a review and what it may find.

Finally, there is a need for an educational research and development effort to create easy-to-deploy-and-access learning opportunities that help K-12 and tertiary level students, the workforce, seniors, strategic policy leaders, government professionals develop critical digital literacies which are defined as: “the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.”<sup>[66]</sup> Such literacies are not new. However, too often, they have been reduced to matters of computer “hygiene habits” updating virus protections and Google searches. New learning experiences are needed for wide-scale implementation that focus on helping voters and users in cyberspace significantly heighten their acuties and skills to evaluate the quality, rigor of information and how their cognitive biases can be taken advantage of. As Allcott and Gentzkow observe and quote: “...the social return to education includes cognitive abilities that better equip citizens to make informed voting decisions. For example, Adam Smith (1776),” The

more [people] are instructed, the less liable they are to the delusions of enthusiasm and superstition, which, among ignorant nations, frequently occasion the most dreadful disorders.”<sup>[67]</sup> 

## NOTES

1. Office of the Director of National Intelligence, (2017, January 06), *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution* (Washington D.C.).
2. As Rogers and Tyushka summarize the goals being pursued by Russia’s “strategic narrative offensive” as seeking to: 1) ‘desynchronise’ political developments in the European Neighborhood to ‘distort’ European perceptions of reality; 2) ‘de-articulate’ the West, i.e., splitting the Atlantic democracies from the European mainland; and 3) ‘saturate’ the vacuum with false and fictitious narratives, to sow confusion and maintain manageable disorder. James Rogers and Andriy Tyushka, (2017, March) “‘Hacking’ into the West: Russia’s ‘Anti-hegemonic’ Drive and the Strategic Narrative Offensive” *Defence Strategic Communications* Vol. 2, 35, <https://www.stratcomcoe.org/james-rogers-andriy-tyushka-hacking-west-russias-anti-hegemonic-drive-and-strategic-narrative>, accessed on May 12, 2017.
3. The Russian influence campaign activities and tactics are well explored in a number of research reports and testimonies; for example, Braden R. Allenby, (2017, Summer), “The Age of Weaponized Narrative or, Where Have you Gone, Walter Cronkite?” *Issues in Science and Technology* (2 and 4), 65-70; Chengcheng Shao, e.al. (2017, July 24), “The Spread of Fake News by Social Bots” (<https://arxiv.org/abs/1707.07592>) (Accessed on July 25, 2017); Clint Watts (March 30, 2017), “Clint Watts’ Testimony: Russia’s Info War on the U.S. Started in 2014. The Daily Beast, <http://www.thedailybeast.com/clint-watts-testimony-russias-info-war-on-the-us-started-in-2014>, accessed on July 18, 2017; Watts, Clint, (2017, April 27) “Inside Russia’s Fake News Playbook” The Daily Beast, <http://www.fpri.org/article/2017/05/inside-russias-fake-news-playbook/>, accessed on July 18, 2017; *ibid.*, Howard Bradshaw, 2017; Edward Lucas and Peter Pomeranzen, (2016, August) *Winning the Information War – Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe* (Washington D.C., Center for European Policy Analysis), [https://cepa.ecms.pl/files/?id\\_plik=2773](https://cepa.ecms.pl/files/?id_plik=2773), accessed on May 9, 2017; Heather A. Conley, et.al., (2016, October) *The Kremlin Playbook – Understanding Russian Influence in Central and Eastern Europe* (Washington D.C. Center for Strategic and International Studies, <https://www.csis.org/analysis/kremlin-playbook>, accessed on May 10, 2017); Shawn Powers and Markos Kounalakis, (Eds.) (2017, May) *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers and Disinformation* (Washington D.C. U.S. Department of State, Advisory Commission on Public Diplomacy), <https://www.state.gov/documents/organization/271028.pdf>, accessed on May 10, 2017; Martin Kragh and Sebastian Asberg, (2017) “Russia’s Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case” *Journal of Strategic Studies*; Published online January 5, 2017; Schreier, (2012) *On Cyberwarfare* (Geneva Centre for the Democratic Control of Armed Forces), <http://www.dcaf.ch/Publications/On-Cyberwarfare>, accessed on June 12, 2017; Brad Allenby and Joel Garreau (2017) *Weaponized Narrative: The New Battlespace* (Arizona State University, Center on the Future of War), <https://weaponizednarrative.asu.edu/publications/weaponized-narrative-new-battlespace>, accessed on July 24, 2017; Alice Marwick and Rebecca Lewis (2017, May) *Media Manipulation and Disinformation Online* (New York, Data and Society Institute), <https://datasociety.net/output/media-manipulation-and-disinfo-online/>, accessed on July 10, 2017; Emerson T. Brooking and P.W. Singer (2016, November) “War Goes Viral—How Social Media is Being Weaponized” *The Atlantic* 318, 4, 70-83; Ferrara, Emilio, et.al., (2015), “The Rise of Social Bots” *Communications of the ACM* 59, 7, 96-104, <https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext>, accessed on June 12, 2017; Alessandro Bessi and Emilio Ferrara (2016, November) “Social Bots Distort the 2016 U.S. Presidential Election Online Discussion” *First Monday* 21, 11, <http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653>, accessed on July 15, 2017; Janus Bugajski, (2017), “The Geopolitics of Disinformation” (Centre for European Policy Analysis), <http://www.infowar.cepa.org/The-geopolitics-of-disinformation>, accessed on June 20, 2017; Sergey Sanovich, (2017), *Computational Propaganda in Russia: The Origins of Digital Misinformation* (Oxford, Oxford University Internet Institute, Working Paper No. 2017.3), <http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-in-russia-the-origins-of-digital-misinformation/>, accessed on July 17, 2017; Matthew Ingram (2017, May 31), “Trump’s Fake Twitter Following Climbs, Sparking Fears of a Bot War” *Fortune Magazine*, <http://fortune.com/2017/05/31/trump-twitter-bot-war/>, accessed on July 17, 2017; Dhiraj Murthy, et.al. (2016) “Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital” *International Journal of Communication* 10, 4952–4971; Christopher Paul and Miriam Matthews () The Russian “Firehose of Falsehood” Propaganda Model Why It Might Work and Options to Counter It” *Rand Perspectives*, [http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND\\_PE198.pdf](http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf); Rand Waltzman, (2015, September) The Weaponization of the Information Environment” *American Foreign Policy Council Defense Technology Program Brief* No. 12, 4-9.

4. Phillip Howard (2017, July 14), *Troops, Trolls and Trouble-Makers: A Global Inventory of Organized Social Media manipulation* (Oxford, Oxford Internet Institute), <https://www.oii.ox.ac.uk/blog/troops-trolls-and-troublemakers-a-global-inventory-of-organized-social-media-manipulation/>, accessed on August 14, 2017.
5. Peter Pomerantsev and Michael Weiss, (2014) *The Menace of Unreality: How the Kremlin Weaponizes Information, culture and Money* (Washington D.C. Institute of Modern Russia, <http://www.interpretermag.com/wp-content/uploads/2015/07/PW-31.pdf>, 4.
6. <https://www.collinsdictionary.com/us/dictionary/English/blind-spot>, accessed on October 29, 2017.
7. Steven Morgan, (2016, June 15), “Cybersecurity spending outlook: \$1 trillion from 2017 to 2021” *CSO Online*, <https://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html>, accessed on November 12, 2017.
8. See for example, Accenture, (2017) *2017 Cost of Cyber Crime Study*, [https://www.accenture.com/t20170926T072837Z\\_w\\_/us-en/\\_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf](https://www.accenture.com/t20170926T072837Z_w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf), accessed on November 28, 2017.
9. The White House, (2013, February 12), Presidential Policy Directive 21– Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>, accessed on October 9, 2017.
10. U.S. Department of Homeland Security, General Services Agency, (2015), *Government Facilities Sector-Specific Plan*, Annex to National Infrastructure Protection Plan 2013), 1, <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf>, accessed on October 12, 2017.
11. <https://en.oxforddictionaries.com/definition/infrastructure>, accessed on November 28, 2017.
12. Larry Diamond, (2004), “What is Democracy?” (Lecture at Hilla University for Humanistic Studies), <http://web.stanford.edu/~ldiamond/iraq/WhatsDemocracy012004.htm>, accessed on November 28, 2017.
13. Secretary of Homeland Security Mr. John Kelly, (2017, June 13), Letter to The Honorable Claire McCaskill, Committee on Homeland Security and Government Affairs, U.S. Senate. Kelly goes on to note: “DHS, in coordination with partners from the Intelligence Community, federal law enforcement, and MS-ISAC, observed Russian cyber actors attempting to access voter registration databases prior to the 2016 elections . . . Based on the observed threat, DHS focused its efforts on providing election officials with information to protect their internet-connected election infrastructure, such as voter registration databases, election websites that provided information for voters on where to find their polling places, and election night reporting systems.” Here again, the focus was on access to voter registration data bases, not access to voter’s beliefs, information, etc.
14. Armed Services Committee, Subcommittee on Cybersecurity, (2017, April 27), *The Weaponization of Information – the Need for Cognitive Security* (Testimony: Rand Waltzman), CT-473, Senate.
15. Peter Roberts, (2017, February/March) “Designing Conceptual Failure in Warfare – The Misguided Path of the West” *RUSI Journal*, 162, 1, 17-19.
16. John Gooch, (ed.), (1997, September) *The Origins of Contemporary Doctrine* (Camberley, Surrey, Strategic and Combat Studies Institute, Occasional Paper no. 30), 5.
17. Quoted in Charles Grant (1997), “The Use of History in the Development of Contemporary Doctrine” in John Gooch (ed.), (1997, September), *The Origins of Contemporary Doctrine* (Camberley, Surrey, Strategic and Combat Studies Institute, Occasional Paper no. 30), 10.
18. Justin Kelly and Mike Brennan, (2009, September), *Alien: How Operational Art Devoured Strategy* (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute Publication 939), <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=939>, accessed on December 1, 2017.
19. Justin Kelly and Mike Brennan, (2009, September), *Alien: How Operational Art Devoured Strategy* (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute Publication 939), <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=939>, accessed on December 1, 2017, 4.
20. Colin S. Gray, (2013, April), *Making Strategic Sense of Cyber Power; Why The Sky is Not Falling*” (Carlisle PA., U.S. Army War College, Strategic Studies Institute Publication No. 1147, <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1147>, accessed on December 1, 2017, 7.

21. Defined here in U.S. military doctrine as: “Cyberspace Operations are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace . . . The successful execution of CO requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment. CO missions are categorized as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN based on their intent. OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.” U.S. Joint Staff, (2013, February 3), **Cyberspace Operations** (Joint Publication 3-12(R)), vii. It is interesting to note that in testimony to the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities in May 2017, CYBERCOM Commander Admiral Rogers’ assessment of the “Cyber Threat Environment” only one sentence or less than 4% of the text was devoted to state-sponsored information influence campaigns with no mention of the Russian influence campaign. By contrast, nearly 20% of the assessment was devoted to the non-state ISIS influence campaign, with the remaining 75% of the threat assessment being devoted to threats to cyber networks and systems, <https://armedservices.house.gov/legislation/hearings/fiscal-year-2018-budget-request-us-cyber-command-cyber-mission-force-support>, accessed on December 1, 2017.
22. Defined here in U.S. military doctrine as: “Information Operations as the integrated employment, during military operations, of Internet-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. U.S. Joint Staff (2014, November 20) **Information Operations** (Joint Publication 3-13), ix.
23. Susan L. Gough, (2003, April 7), **The Evolution of Strategic Influence** (Carlisle Barracks, PA, U.S. Army War College, USAWC Strategy research Project), 1.
24. Even Department-level strategy documents, most particularly the Department of Defense Strategy for Operations in the Information Environment, <https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf>, accessed on October 15, 2017, contain “operations” to a military operational context focused around supporting Joint Force Commanders. While similar references occur in most doctrine statements, and take as an example, the U.S. Marine Corps definition of information operations: “Information Operations is the integration, coordination and synchronization of all actions take in the information environment to affect a target audience’s behaviour in order to create an operational advantage for the commander”, <http://www.quantico.marines.mil/Tenants/Marine-Corps-Information-Operations-Center/>, accessed on October 15, 2017.
25. Narrative power defined “...a vehicle for manipulating individuals so that they are more inclined to do what you want, not because you have forced them to but because you have convinced them that they want to do what you want them to.” (Brandon R. Allenby (2017, Summer) “The Age of Weaponized Narrative or Where Have You Gone, Walter Cronkite?” **Issues in Science and Technology**, 66, <http://issues.org/33-4/the-age-of-weaponized-narrative-or-where-have-you-gone-walter-cronkite/>, accessed on September 10, 2017.
26. Peter Roberts, (2017, February/March) “Designing Conceptual Failure in Warfare – The Misguided Path of the West” **RUSI Journal**, 162, 1, 18.
27. For a treatment of all the different sources of soft power, see Giulio M. Gallarotti, (2015), “Smart Power: Definitions, Importance and Effectiveness” **Journal of Strategic Studies** 38:3, 249.
28. Mark Leonard, (2016, January) “Weaponising Interdependence” in Mark Leonard (ed.), **Connectivity Wars – Why Migration, Finance and Trade are the Geo-Economic Battlefields of the Future** (European Council on Foreign Relations), 13, <http://www.ecfr.eu/europeanpower/geoeconomics>, accessed on November 7, 2017.
29. U.S. Department of Defense, (2015), **The Department of Defense Cyber Strategy**, Washington D.C., [https://www.defense.gov/News/Special-Reports/0415\\_Cyber-Strategy/](https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/), accessed on November 30, 2017.
30. See for example: Samanth Subramanian, (2017, February), “Inside the Macedonian Fake News Complex” **Wired Magazine**, <https://www.wired.com/2017/02/veles-macedonia-fake-news/>, accessed on October 24, 2017; Samantha Bradshaw and Philip Howard (2017) **Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation** (Oxford, Oxford Internet Institute, Computational Propaganda Research Project Working Paper 12), <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>, ccessed on August 12, 2017; Andrei

- Soldatov, (2017, February-March) "Putin's Private Hackers' *The World Today* (London, Chatham House), <https://www.chathamhouse.org/system/files/publications/twt/Putin%E2%80%99s%20private%20hackers%20Soldatov.pdf>, accessed on June 12, 2017; Keir Giles, (2015, August-Sept) "Putin's Troll Factories" *The World Today* Vol. 71, No. 4 (London, Chatham House), <https://www.chathamhouse.org/publication/twt/putins-troll-factories>, accessed on 12 October 12, 2017, Nichole Einbeinder, (2017, November 1), "The Election is Over, But Russian Disinformation Hasn't Gone Away" *PBS Frontline*, <https://www.pbs.org/wgbh/frontline/article/the-election-is-over-but-russian-disinformation-hasnt-gone-away/>, accessed on November 12, 2017.
31. Nazli Choucri, (2012), *Cyberpolitics in International Relations* (Cambridge Mass, MIT Press), 4.
32. Bernard Brodie, (1959), *Strategy in the Missile Age* (Santa Monica, The Rand Corporation, Report R-335).
33. Clayton Christensen, (2013), *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Cambridge, Mass., Harvard Business Review Reprint, Reprint Edition).
34. This is seen, for example, in the Obama Administration's "Third Off-set Strategy", confirmed in mid-2017 in the Office of Management and Budget Memorandum on R&D priorities for FY 2019. The third offset strategy was designed to "'offset' potential competitors as they reach parity with the United States in some critical area." It was established to recognize that; "Adversaries are devising ways to counter our technological over-match. So across the board, we see rapid developments in nuclear weapons, modernization of nuclear weapons, new anti-ship, anti-air missiles; long-range strike missiles; counter-space capabilities; cyber capabilities, electronic warfare capabilities; special operations capabilities that are operated at the lower end. All are designed to counter our traditional military strengths and our preferred way of operating." Pellerin, Cheryl, (2016, October 31), "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence" *DoD News*, U.S. Department of Defense, Defense Media Activity), <https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/>, accessed on November 30, 2017; Also see: U.S. Office of Management and Budget Memorandum (2017, August 17), FY 2019 Administration Research and Development Budget Priorities (M-17-30), <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-30.pdf>, accessed on November 30, 2017.
35. Xenios Thrasyvoulou, (2014, December), "Understanding the Innovator's Dilemma" *Wired Magazine*, <https://www.wired.com/insights/2014/12/understanding-the-innovators-dilemma/>, accessed on November 30, 2017.
36. Christopher Paul and Miriam Matthews, (2016) *The Russian "Firehose of Falsehood" Propaganda Model Why It Might Work and Options to Counter It* (Santa Monica CA, Rand Corporation PE-198-OSD), <https://www.rand.org/pubs/perspectives/PE198.html>, accessed on August 3, 2017.
37. Alexander Klimberg, (2017, July), *The Darkening Web – The War for Cyberspace* (New York, Penguin Press), 2; Council on Foreign Relations Fellow, Gordon Goldstein summarized Klimberg's view: the "... internet has become an arena for [an]...international security competition fought in an increasingly Hobbesian ecosystem of digital aggression and overt information warfare." Gordon M. Goldstein, (2017, August 4), "How Enemy States do Battle in Cyberspace" *Washington Post Book Review*, [https://www.washingtonpost.com/opinions/how-enemy-states-do-battle-in-cyberspace/2017/08/04/0bb43914-672f-11e7-8eb5-cbccc2e7bfbf\\_story.html?utm\\_term=.01e76da8a88b](https://www.washingtonpost.com/opinions/how-enemy-states-do-battle-in-cyberspace/2017/08/04/0bb43914-672f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.01e76da8a88b), accessed on October 10, 2017.
38. Barack Obama, (2015) *National Security Strategy* (Washington D.C. The White House), [https://obamawhitehouse.archives.gov/sites/default/files/docs/2015\\_national\\_security\\_strategy\\_2.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf), accessed on August 10, 2017, 8.
39. Braden R. Allenby, (2017, Summer), "The Age of Weaponized Narrative or Where Have You Gone, Walter Cronkite?" *Issues in Science and Technology*, 66, <https://weaponizednarrative.asu.edu/publications/age-weaponized-narrative>, accessed on September 24, 2017. This fits with the Russian Ministry of Defence's 2011 Conceptual Views on the Activities of the Armed Forces of the Russian federation in Information Space, quoted by Timothy Thomas, as active measures to: "undermine political, economic and social systems, carry out mass psychological campaigns against the population of a State in order to destabilize society and the government; and force a State to make decisions in the interests of their opponents." Thomas, Timothy, (2016, February 17) "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations" *Defence Strategic Communications* Vol. 1, 11, <https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations>, accessed on 4 April 2017. In this, Russian strategists have taken a leaf from war-strategist Sun Tzu's axioms, most particularly: (1) *supreme excellence consists in*



breaking the enemy's resistance without fighting; (2) You can be sure of succeeding in your attacks if you only attack places which are undefended; and (3) If your enemy . . . is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant . . . If his forces are united, separate them. If sovereign and subject are in accord, put division between them. Attack him where he is unprepared, appear where you are not expected." See <https://suntzusaid.com/>, accessed on December 2, 2017; and Eric Jackson, (2014, May 23), "Sun Tzu's 31 Best Pieces of Leadership Advice" *Forbes Magazine*, <https://www.forbes.com/sites/ericjackson/2014/05/23/sun-tzus-33-best-pieces-of-leadership-advice/#748c2ea5e5e>, accessed on December 2, 2017.

40. Brad Allenby, (2017, June), "What's New About Weaponized Narrative? White Paper for the U.S. National Academy of Sciences" (Arizona State University, Weaponized Narrative Initiative), <https://weaponizednarrative.asu.edu/publications/weaponized-narrative-white-paper-0>, accessed on September 12, 2017.

41. For example, in Charles Kriel's review essay, he notes: "According to Grassegger and Kroegerus, Cambridge Analytica divided America into 32 personality types for the Trump Campaign, and focused on seventeen states . . . The company's psychometric findings told the Trump Team which messages were working and where . . . One hundred-and-seventy-five thousand algorithmically-generated variations were designed not only to get out the vote, but to suppress it as well." [emphasis added] Charles Kriel, (2017, Autumn), "Fake News, Fake Wars, Fake Worlds" *Defence Strategic Communications* 3, <https://www.stratcomcoe.org/charles-kriel-fake-news-fake-wars-fake-worlds>, accessed on December 2, 2017). See also: Illing, Sean (2017, Oct 22), "Cambridge Analytica, the Shady Data Firm that Might be a Key Trump-Russia Link, Explained", <https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-trump-kushner-flynn-russia>, accessed on October 22, 2017). See also Nicholas Fandos, Cecilia Kang, Mike Isaac (2017, November 1), "House Intelligence Committee Releases Incendiary Russian Social Media Ads." *New York Times*, <https://www.nytimes.com/2017/11/01/us/politics/russia-technology-facebook.html>, accessed on November 4, 2017. Also in this context can be considered the Twitter posts that were designed to gull voters into believing that sending a text message would record their vote. This voter suppression tactic was revived in the late 2017 Virginia Gubernatorial election. O'Sullivan, Donnie (2017, November 8), "Virginia Voter Suppression Tweets went Undetected by Twitter for Hours, <http://money.cnn.com/2017/11/07/media/twitter-virginia-voter-suppression/index.html>, accessed on December 2, 2017.

42. Simon Kemp (2017, January 24), *Digital in 2017: Global Overview* (WeareSocial.Hootsuite), <https://wearesocial.com/special-reports/digital-in-2017-global-overview>, accessed on December 2, 2017.

43. Pew Research Center (2017, January 12) *Social Media Fact Sheet*, <http://www.pewinternet.org/fact-sheet/social-media/>, accessed on 12 August 2017; and Elisa Shearer and Jeffrey Gottfried, (September 1, 2017), *News Use Across Social Media Platforms 2017* (Pew Research Center), <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>, accessed on September 30, 2017.

44. See <https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=814>, accessed on November 22, 2017, and Kathleen Chaykowski (2017, October 31) "Highlights From Facebook's, Twitter's First Senate Hearing On Russian Meddling" *Forbes Magazine*, <https://www.forbes.com/sites/kathleenchaykowski/#4f136f241eal>, accessed on November 10, 2017.

45. Issie Lapowsky, (2017, November 1), "Eight Revealing Moments from the Second Day of Russia Hearings" *Wired Magazine*, <https://www.wired.com/story/six-revealing-moments-from-the-second-day-of-russia-hearings/>, accessed on November 10, 2017.

46. See for example: Senate Armed Services Subcommittee on Cybersecurity, (2017, April 27), *The Weaponization of Information – the Need for Cognitive Security* (Testimony: Rand Waltzman), CT-473, Senate; and Kelly Born, (2017, October 9) "Six Features of the Disinformation Age" *Stop Fake*, <https://www.stopfake.org/en/six-features-of-the-disinformation-age/>, accessed on December 2, 2017.

47. See for example, Seth Flaxman, Sharad Goel, Justin M. Rao, (2016) "Filter Bubbles, Echo Chambers and Online News Consumption" *Public Opinion Quarterly*, 80, Special Issue, 298–320; and Freedom House, (2017, November 9) *Freedom on the Net 2017 – Manipulating Social Media to Undermine Democracy*, <https://freedomhouse.org/report/freedom-net/freedom-net-2017>, accessed on December 2, 2017.

48. Keir Giles, (2016, May 20), "The Next Phase of Russian Information Warfare" *Defence Strategic Communications*, <https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles>, accessed on April 4, 2017.

49. See for example, Bob Schieffer with H. Andrew Schwartz, (2017) *Overload – Finding the Truth in Today's Deluge of News* (Lanham MD, Rowman and Littlefield, Center for Strategic and International Studies).

50. Christophe Paul and Miriam Matthews, The Russian “Firehose of Falsehood” Propaganda Model Why It Might Work and Options to Counter It” *Rand Perspectives*, [http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND\\_PE198.pdf](http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf), accessed on November 12, 2017.
51. See Tom Becka’s Ted Talk, (2017, March 14) *The Real News about Fake News*, <https://www.youtube.com/watch?v=U-w6QdzUpvo>, accessed on September 27, 2017, where he remarks: “It’s easier to fool someone than to convince them they were fooled.” And “How easy it is to make people believe a lie . . . And how hard it is to undo that work again.”
52. Pew Research Center, (October, 2017) “The Partisan Divide on Political Values Grows Even Wider”, <http://www.people-press.org/2017/10/05/the-partisan-divide-on-political-values-grows-even-wider/>, accessed on December 3, 2017.
53. Tim Wu, (2016) *The Attention Merchants – The Epic Scramble to get Inside Our Heads* (New York, Knopf).
54. See for example, Bryan Gardiner, (2015, December 18), “You’ll Be Outraged at How Easy it was to Get You to Click on This Headline” *Wired Magazine*, <https://www.wired.com/2015/12/psychology-of-clickbait/>, accessed on November 9, 2017.
55. See for example, Julio Reis, Fabricio Benevenuto, Pedro O.S. Vaz de Melo, Raquel Prates, Haewoon Kwak and Jisun An, (2015, April 6) “Breaking the News: First Impressions Matter on Online News” Paper presented to the 2015 International AAAI Conference on Web and Social Media, <https://arxiv.org/abs/1503.07921>, accessed on November 12, 2017; and Emilio Ferrara and Zeyao Yang, (2015, November 6), “Measuring Emotional Contagion in Social Media” *PLoS One* 10 (11), <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0142390>, accessed on November 12, 2017.
56. Hunt Allcott and Matthew Gentzkow (2017) *Social Media and Fake News in the 2016 Election* (National Bureau of Economic Research, Working Paper No. 23089), <http://www.nber.org/papers/w23089>, accessed on October 9, 2017, 3.
57. See for example, Ben Nimmo and Nika Aleksejeva, (2017, March 23), “Busting Fakes, Kremlin Style (Part 1) Fact checking the Russian Foreign Ministry’s “fakes” page” The Atlantic Council, Digital Forensic Research Lab, <https://medium.com/dfrlab/busting-fakes-kremlin-style-part-1-6bc4369d89e3>, accessed on December 2, 2017.
58. See for example, Daniel Drezner, (2017) *The Ideas Industry: How Pessimists, Partisans, and Plutocrats are Transforming the Marketplace of Ideas* (Oxford, Oxford University Press), and Peter Overby (2017, September 20), “Who Controls Think Tanks? Shift In Funding Highlights Changes In The Industry” *National Public Radio*, <https://www.npr.org/2017/09/20/551364067/who-controls-think-tanks-shift-in-funding-highlights-changes-in-the-industry>, accessed on December 4, 2017.
59. See for example, Portia Roelofs and Max Gallien (2017, September 19) “Clickbait and impact: how academia has been hacked,” <http://blogs.lse.ac.uk/impactofsocialsciences/2017/09/19/clickbait-and-impact-how-academia-has-been-hacked/>, accessed on November 24, 2017.
60. John C. Camillus, (2008, May) “Strategy as a Wicked Problem” *Harvard Business Review*, <https://hbr.org/2008/05/strategy-as-a-wicked-problem>, accessed on December 14, 2017.
61. The Smith-Mundt Act of 1948, amended in 1972 and 1998, prohibits the US government from “propagandizing” the American public with information and psychological operations directed at foreign audiences; some modifications have been made in President Reagan’s NSD-77 in 1983, President Clinton’s PDD-68 in 1999, and President Bush 43’s NSPD-16 in July 2002.
62. Alexander Klimberg, (2017, July), *The Darkening Web – The War for Cyberspace* (New York, Penguin Press), 3.
63. Peter Diamandis, (2016, November 7) “5 Big Tech Trends that will make this Election Look Tame” *Singularity Hub*, <https://singularityhub.com/2016/11/07/5-big-tech-trends-that-will-make-this-election-look-tame/#sm.00000wnbp-0molve50u4pupplbcuw>, accessed on November 12, 2017; see also, Lee Rainie and Janna Anderson, (2017, February 8), *Code Dependent: pros and Cons of the Algorithm Age* (Pew Research Center, <http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/>), accessed on November 12, 2017.
64. See for example, Metz, Rachel (2017, October 19), “Smartphones Are Weapons of Mass Manipulation” *MIT Review*, <https://www.technologyreview.com/s/609104/smartphones-are-weapons-of-mass-manipulation-and-this-guy-is-declaring-war-on-them/>, accessed on November 7, 2017.
65. Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari, Andrej Zwitter, (2017, February 25) “Will Democracy Survive Big Data and Artificial



Intelligence?” *Scientific American*, <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>, accessed on 12 December 2017.

66. Liana Heitin, (2016, November 8), “Digital Literacy: An Evolving Definition” *Education Week*, <https://www.edweek.org/ew/articles/2016/11/09/what-is-digital-literacy.html>, accessed on December 15, 2017.

67. Hunt Allcott and Matthew Gentzkow (2017) *Social Media and Fake News in the 2016 Election* (National Bureau of Economic Research, Working Paper No. 23089), <http://www.nber.org/papers/w23089>, accessed on October 9, 2017, 3.

# The Strategic Support Force and the Future of Chinese Information Operations

---

Elsa B. Kania

John K. Costello

The establishment of the Strategic Support Force (战略支援部队, SSF) in December 2015 was a critical milestone in the history of the Chinese People's Liberation Army (PLA), against the backdrop of its historic reform agenda.<sup>[1]</sup> The SSF's creation reflects an innovation in force structure that could allow the PLA to operationalize its unique strategic and doctrinal concepts for information operations. Despite limited transparency, it is nonetheless possible to glean critical details about the SSF's composition and key missions, based on a range of open sources.<sup>[2]</sup> It is clear that the SSF has been designed as a force optimized for dominance in space, cyberspace, and the electromagnetic domain, which are considered critical "strategic commanding heights" for the PLA.<sup>[3]</sup> Under its Space Systems Department (航天系统部), the SSF has seemingly consolidated control over a critical mass of the PLA's space-based and space-related assets. Through these capabilities, the SSF has taken responsibility for strategic-level information support (信息支援) for the PLA in its entirety, enhancing its capability to engage in integrated joint operations and remote operations.<sup>[4]</sup> Concurrently, the SSF has integrated the PLA's capabilities for cyber, electronic, and psychological warfare into a single force within its Network Systems Department (网络系统部), which could enable it to take advantage of key synergies among operations in these domains. However, beyond the SSF, the PLA also appears to be building up network-electronic operations (网电作战) capabilities within its national Joint Staff Department headquarters and within new regional theater commands (战区), reflecting the emergence of a multi-level force structure specializing in information operations. Thus, the SSF reflects the PLA's uniquely integrated approach to force structure and operations in these vital new domains. This realization of this paradigm through the SSF will enhance the PLA's capabilities to fight and win future "informatized" (信息化) wars.

©2017 Elsa Kania, John Costello



Elsa B. Kania is an adjunct fellow with the Technology and National Security Program at the Center for a New American Security, where she focuses on Chinese defense innovation in emerging technologies, particularly artificial intelligence. Her research interests include Chinese military modernization, information warfare, and defense science and technology. She is an independent analyst, consultant, and co-founder of the China Cyber and Intelligence Studies Institute (CCISI), which seeks to become the premier venue for analysis and insights on China's use of cyber and intelligence capabilities as instruments of national power.

### *The Impetus for Reforms*

The creation of the SSF reflects the PLA's attempts to resolve prior issues and build up its military cyber forces to ensure their combat capability. Although critical elements of Chinese thinking on information operations had crystallized by the late 1990s—and have remained remarkably consistent since—the PLA has lagged in its efforts to construct forces capable of realizing the intended missions and strategic objectives.<sup>[5]</sup> Instead, China's military cyber force often ended up being turned to purposes of political and commercial cyber espionage, whether in furtherance of formal missions or, in some cases, seemingly for profit and/or at the behest of local state-owned enterprises. Even when those activities were sanctioned by the appropriate command authorities, the scope and scale may not have been fully known to higher-level PLA leadership, while the risks of apprehension appear to have been largely dismissed, due to the perception that attribution would be futile.

However, this calculus has since changed. In February 2013, Mandiant released the APT1 report, which exposed Unit 61398 of the PLA,<sup>[6]</sup> and then, in May 2014, the US government charged five 3PLA officers with computer hacking and economic espionage.<sup>[7]</sup> Although this intended 'naming and shaming' has not resulted in a complete cessation of such activities, their exposure does appear to have had, to at least a limited extent, a deterrent effect and resulted in discernible changes in PLA behavior, including an initial reduction in the frequency of its cyber espionage activities. In September 2015, Presidents Obama and Xi agreed, "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."<sup>[8]</sup>



John Costello is a Senior Analyst for Cyber and East Asia at Flashpoint. John is a co-founder and the executive director of the China Cyber and Intelligence Studies Institute. He is a Cybersecurity Fellow for New America and former Congressional Innovation Fellow for majority staff in the U.S. House of Representatives Committee on Oversight and Government Reform. John is also a US Navy veteran, former NSA Analyst, and is fluent in Mandarin Chinese.

Subsequently, there was a notable decrease in Chinese Advanced Persistent Threat (APT) activity, as documented by FireEye, among others.<sup>[9]</sup>

At this point, it appears that there has been a notable change in the pattern of Chinese cyber operations. There have been several incidents of cyber-enabled intellectual property theft by Chinese APT groups, although some have seemingly reflected notional adherence to the agreement by targeting companies specializing in defense technology, telecommunications, and software services that could be utilized for both legitimate defense and commercial purposes. Concurrently, the activities of non-military cyber actors, especially a number of contractors linked to the Ministry of State Security (MSS), have become more prominent, while military cyber forces appear to have been redirected away from such activities. For instance, in November 2017, three Chinese hackers working for Boyusec, which is known to act on behalf of MSS,<sup>[10]</sup> were charged by the US government with hacking several corporations for commercial advantage,<sup>[11]</sup> in apparent violation of the Obama-Xi agreement. It remains to be seen whether the tenuous norm against commercial cyber espionage will take hold.<sup>[12]</sup> In the meantime, the MSS appears to have taken the lead, emerging as a major player and full-spectrum intelligence agency, while the focus of PLA cyber operations seems to have shifted away from commercial towards combat-oriented activities.

China's government has also actively sought to build up a cyber defense at the national level, mainly in response to a series of incidents—including the discovery of Stuxnet, the Arab Spring, and the Snowden—each of which revealed unique threats and vulnerabilities that China faces in the cyber domain. The resulting concerns over

pervasive information insecurity have resulted in the development of a more robust framework to enhance national security and resilience. Consequently, China has undertaken a complete overhaul of legal and regulatory regime overseeing information security, spearheaded by the Cyberspace Administration of China (CAC), founded in 2014. The key component of this information security push is the National Cybersecurity Law (NCL), which was made law in November 2016 and implemented in June 2017. The law has acted as a central organizing principle and enforcement mechanism under which agencies have implemented new regulatory regimes over content management, device management, cybersecurity information sharing, encryption, and supply-chain security.<sup>[13]</sup>

Concurrently, the PLA's historic reform agenda has sought to transform it into a "world-class" military capable of "fighting and winning wars," which requires the advancement of offensive cyber capabilities that would be integral in early stages of a conflict. As constituted, PLA cyber forces were deemed inadequate relative to superior US cyber capabilities. The separation of cyber espionage and offensive cyber forces between 3PLA and 4PLA seemingly prevented their realization as a coherent, integrated fighting force for this new domain. On the surface, the creation of the SSF could be seen as a response and parallel to the US establishment of U.S. Cyber Command (USCYBERCOM).<sup>[14]</sup> However, a deeper analysis reveals that a more apt counterpart may be USCYBERCOM's parent organization, U.S. Strategic Command (USSTRATCOM), which, like the Strategic Support Force, is responsible for space, cyber operations, and strategic C4ISR support to "combatant commands", regional joint-force areas of responsibility that act has direct analogs to the Chinese military's new theater commands. The SSF is nevertheless a uniquely divergent entity in force structure that distinguishes itself from both USSTRATCOM and USCYBERCOM in several key respects. The most obvious is that China's Strategic Support Force is a military service rather than joint force command and lacks a nuclear mission, USSTRATCOM's original *raison d'être*. For cyber operations, the differences are deeper and more qualitative. The SSF's cyber corps approach the cyber domain in a much more comprehensive way, reflecting a highly integrated approach to information operations that actualizes critical concepts from PLA strategic and doctrinal approaches.

### ***Overview of Force Structure***

The SSF is a unique product of the PLA's reforms, which seek to enhance its capabilities to engage in joint operations.<sup>[15]</sup> In its design, the SSF is intended to be optimized for future warfare, in which the PLA anticipates such "strategic frontiers" (战略边疆) as space, cyberspace, and the electromagnetic domain will be vital to victory.<sup>[16][17]</sup> According to its commander, Lieutenant General Gao Jin (高津), the SSF will "protect the high frontiers and new frontiers of national security," while seeking to "seize the strategic commanding heights of future military competition."<sup>[18]</sup> Despite its relative novelty, the SSF itself is constructed from prior organizational components, reflecting a modular approach to reorganization through which existing institutions have been restructured under new organizations to align with new paradigms.

The SSF is largely composed of operational units and organizations from the PLA's former four "general departments", the General Staff Department (GSD), General Armaments Department (GAD), and General Political Department (GPD) units responsible for space, cyber, electronic, and psychological warfare. In its function and structure, the SSF appears to act in a similar status to that of the nuclear-armed PLA Rocket Force's (PLARF) predecessor, the Second Artillery Corps, which similarly consolidated strategic capabilities under direct national control. This environment has served the strategic missiles mission well; in a few decades, China has fielded an impressive array of both nuclear and conventional missiles that now form the bedrock of its nuclear and conventional deterrence posture. Military leadership may be trying to replicate the success of that model in space and cyber domains, responding to shifts in modern warfare by extending concepts of conventional deterrence into these domains.<sup>[19]</sup>

The SSF appears to be designed around the operational imperative of "peacetime-wartime integration," which is also a major impetus for the overall reform agenda.<sup>[20]</sup> Under its prior organizational structure, the PLA would have confronted the challenge of transitioning from a peacetime posture to a wartime posture just prior or immediately after the outbreak of war. For strategic-level information operations, such a shift would have demanded unprecedented coordination across entrenched divisions between national-level departments, services, and military region to form an information operations group (信息作战群) in conflict. The SSF has seemingly streamlined this process through organizing these units into operational groups as standard practice, optimized as a wartime structure. This concept of peacetime-wartime integration is particularly critical for the SSF's Network Systems Department and cyber mission. At a basic level, cyber operations require a persistent cycle of cyber reconnaissance, capabilities development, and deployment to ensure cyber effects can be leveraged in a conflict. Given the functional integration of these peacetime and wartime activities—and the close relationship between reconnaissance and attack—in cyber operations, the integration of China's military cyber offense and espionage capabilities has become a functional necessity.<sup>[21]</sup> This force structure is consistent with the PLA's recognition of the reality of blurred boundaries between peace and warfare in these domains, which is reflected in its notion of "military struggle" (军事斗争) in cyberspace, as confrontation occurring across a spectrum, of which the highest form is warfare.

Concurrently, the SSF is intended to actualize a shift from a discipline-centric to a domain-centric structure that enhances the PLA's capabilities in critical strategic frontiers. Previously, space, cyber, and electronic warfare units were organized according to the type of mission—the disciplines of reconnaissance, attack, or defense—rather than their warfighting domain. This is best seen in the cyber mission, for which espionage was handled by the Third Department of the former GSD (3PLA), while the offensive elements were handled by the Fourth Department (4PLA), and the former Informatization Department

(信息化部) undertook certain elements of defense. Under the SSF, the idea of “integrated reconnaissance, offense, and defense” (侦攻防一体化) may serve as an organizing concept, which could involve the integration of disciplines together to enhance full-spectrum war-fighting capabilities.<sup>[22]</sup> This new organizational structure could also enable levels of unified research and development, planning, force construction, and operations that would have been infeasible under the previous structure.

Concurrently, the SSF will confront the reality of rapid, disruptive technological changes, often driven by research and development in the private sector. These dynamics render the SSF’s tasking to pursue civil-military integration (or “military-civil fusion,” 军民融合) as an integral aspect of its mission. This will involve taking advantage of dual-use technological advances and leveraging civilian talent. Indeed, cyberspace has been highlighted as a priority domain for China’s national military-civil fusion strategy, with a particular focus on personnel training and issues of human capital.<sup>[23]</sup> For instance, the SSF has established partnerships with over nine units and enterprises, such as the University of Science and Technology of China and the China Electronics Technology Group (CETC), to focus on “fostering high-end talent,” including through education, training, cooperation, and exchanges.<sup>[24]</sup>

Similarly, authoritative PLA texts, such as the 2013 AMS SMS, have argued, “since the boundaries between peacetime and wartime are ambiguous, and military and civilian attacks are hard to distinguish, persist in the integration of peace and war [and] in the military-civil fusion; in peacetime, civilians hide the military, [while] in wartime, the military and the people, hands joined, attack together...”<sup>[25]</sup> As prominent PLA strategist Ye Zheng (叶征) highlighted, “The strategic game in cyberspace is not limited by space and time, does not differentiate between peacetime and wartime, [and] does not have a front line and home-front...”<sup>[26]</sup> Indeed, the SSF is designed to achieve dominance in a domain in which traditional boundaries are blurred and in which the private sector is integrally involved.

### ***The SSF’s Leadership, Structure, and Missions***

Established in December 2015, the SSF is commanded by Lieutenant General Gao Jin (高津). Gao Jin served with the former Second Artillery Force and was the president of the Academy of Military Science, which advises the Central Military Commission on strategy and doctrine.<sup>[27][28]</sup> From an operational perspective, the SSF’s headquarters for its space and cyber mission forces are the Space Systems Department (航天系统部) and Network Systems Department (网络系统部) respectively, which command combat forces likely referred to as the “Space Corps” (天军) and “Cyber Corps” (网军). Through the consolidation of the PLA’s strategic-level capabilities for these domains, the Space Systems Department and Network Systems Department will respectively pursue missions of strategic information support and strategic-level information operations.



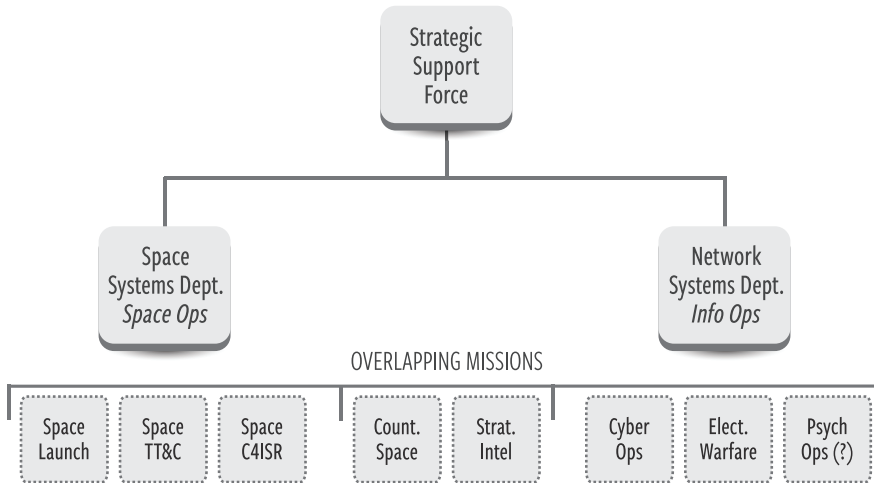


Figure 1. The basic missions of the SSF's two main components: Space and Cyber Corps.

The SSF's Network Systems Department (网络系统部), likely under the command of Major General Zheng Junjie (郑俊杰), appears to integrate a critical mass of the PLA's strategic-level cyber, electronic, and psychological warfare capabilities. The former 3PLA, which was responsible for technical reconnaissance and cyber espionage, appears to be the central component around which the Network Systems Department is organized.<sup>[29]</sup> As the PLA's premiere cyber espionage organization, the 3PLA's preeminence in this domain makes them a natural fit as the primary "tent-pole" for the SSF's cyber force. Although cyber espionage constitutes one of its central missions, the 3PLA has also been responsible for traditional signals and communications intelligence. Not only the former 3PLA's Technical Reconnaissance Bureaus but also the two electronic warfare brigades from the former 4PLA have been integrated into the Network Systems Department.<sup>[30]</sup>

Of note, the Network Systems Department also appears to have taken over essential research agendas that could support capability development. It is noteworthy that the GSD 56th, 57th, and 58th Research Institutes, all formerly under the 3PLA, have all been transferred to the Network Systems Department.<sup>[31]</sup> These research institutes previously reported directly to 3PLA headquarters and were tasked with military research, development, testing, and acquisition (RDT&A) in support of 3PLA's mission.<sup>[32][33]</sup> Also, the 54th Research Institute, which was formerly subordinate to the 4PLA and focused on electronic and network countermeasures, has moved to the SSF.<sup>[34]</sup>

Although the name "Network Systems Department" might imply that the department solely incorporates cyber/network warfare capabilities, it appears that China's view of cyberspace is changing, and this organizational structure reflects such a conceptual evolution. The PLA seems to be starting to redefine what "cyberspace" means, expanding the definition to include all aspects of information warfare, such that the concept is



effectively synonymous with the information domain.<sup>[35]</sup> This would more closely comport with how China's civil authorities view cybersecurity as closely linked to the notion of information security, which includes concerns over content and reflects ideological concerns. In an operational context, this means that China has a more integrated approach to information domain across the "stack," from physical assets, through electronics, to digital networks, all the way to information exchanges and media content. This integrated approach may allow for better planning, acquisition, and operations while enabling the creation of a more flexible cadre of personnel tailored towards new paradigms of information operations.

Although the SSF has consolidated a critical mass of capabilities, the PLA's information operations forces appear to have a more complex, multi-level structure. The SSF does not appear to have incorporated and consolidated the entirety of PLA's cyber espionage and technical reconnaissance capabilities. Under the PLA's previous structure, each service and military region (MR) maintained its own Technical Reconnaissance Bureau (TRB), responsible for signals intelligence and cyber espionage. At this point, it is unclear to what extent the SSF will incorporate these other service or military region TRBs, though there are preliminary indications that a number of them have been transferred into the SSF. On the other hand, the cyber defense mission associated with the former GSD Informatization Department's Information Assurance Base (信息保障基地) and its subordinate Network Security and Defense Center (网络安防中心), remains under the new Joint Staff Department's Information and Communications Bureau (信息通信局).<sup>[36]</sup> Although, the SSF could incorporate or develop a defensive mission to complement its reconnaissance and offensive capabilities, it appears that the Cyberspace Administration of China, along with the Ministry of Public Security, take primary responsibility for supporting cyber defense at the national level, including the protection of critical infrastructure, and regulatory and law enforcement responsibility, respectively, over compliance with cybersecurity laws and provisions.

Surprisingly, the former GSD Fourth Department (4PLA), also known as the Electronic Countermeasure and Radar Department (电子对抗与雷达部), has *not* been transferred in its entirety to the SSF. While its subordinate electronic warfare brigades have been incorporated into the SSF, its headquarters appears to have been shifted under the CMC Joint Staff Department as the Network-Electronic Bureau (网络电子局 or 网电局) and the Network-Electronic Countermeasures *Dadui* (网电对抗大队), with Wang Xiaoming (王晓明) as the head.<sup>[37]</sup> The former 4PLA was previously responsible for the entirety of the strategic-level, or national level, and a considerable element of campaign-level electronic warfare for the PLA. Also of note, there appear to be network-electronic countermeasures (网电对抗) units not only at the CMC level but even under the new theater commands (战区),<sup>[38]</sup> but the parameters of their missions and potential coordination with the SSF remain to be seen.

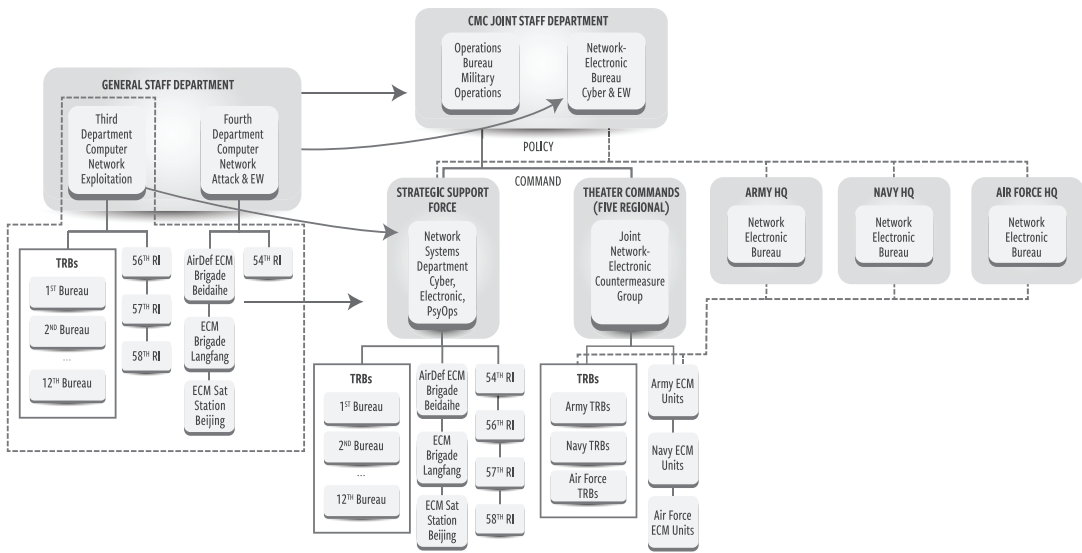


Figure 2. A notional chart depicting the shift in responsibilities for electronic warfare and cyber warfare under the new “network-electronic” paradigm.

At this point, given this complex force structure, there are some unresolved questions regarding command. It appears that the SSF, not unlike the former Second Artillery Force, and now Rocket Force, falls under the direct authority of the CMC rather than being commanded by theater commands. However, the new theater commands and subordinate service elements may possess or construct their own cyber or network-electronic operations capabilities. According to one notional schematic by an SSF scholar, theater command joint operations command departments, through their joint operations cyberspace operations command centers, will exercise command over cyberspace operations forces under each of the services; the CMC Joint Operations Command, through a CMC Joint Command Cyberspace Operations Command Center, commands over the SSF itself, which commands cyberspace strategic reconnaissance, assault, defense, and support forces and capabilities; and in addition, the Cyberspace Administration of China, has authority over military-local cyberspace coordination centers, which could support defensive operations.<sup>[39]</sup> Although this is not necessarily fully consistent with official command structure, the key elements of it reflect a three-tiered approach to China’s cyber capabilities. At present, the construction of more robust cyber or network-electronic combat forces within theater commands likely remains a work in progress. In addition, there do not yet appear to be functional mechanisms for coordination among cyber operations forces at different levels.

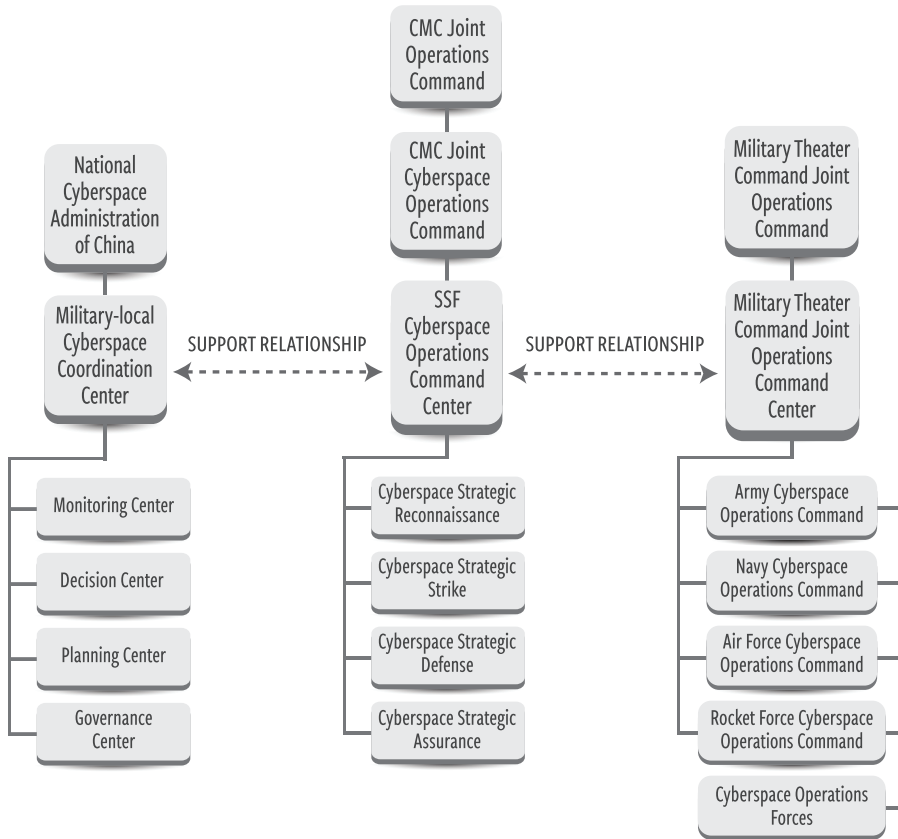


Figure 3. Notional Cyberspace Operational Command System Structure

In addition, PLA information operations forces might be differentiated among strategic information operations forces, which include satellite information attack and defense forces, “new concept” electronic assault forces, and Internet assault forces; campaign information operations forces, which include conventional electronic warfare forces, anti-radiation assault forces, and battlefield cyber warfare forces; and tactical information operation forces, which include satellite information attack and defense forces, and battlefield cyber warfare forces, according to a relatively authoritative PLA textbook.<sup>[40]</sup>

The PLA’s force structure for network-electronic operations capabilities must be contextualized by the concept of the information operations group (信息作战), a joint-force wartime construct that was displayed during the August 2017 military parade that marked the 90th anniversary of the PLA’s establishment.<sup>[41]</sup> In the parade, the information operations group included an information support formation (信息支援方队), electronic reconnaissance formation (电子侦察方队), electronic countermeasures formation (电子对抗方队), and unmanned aerial vehicles (UAV) formation (无人机方队).<sup>[42]</sup> The informa-

tion operations group would bring together the disparate elements responsible for cyber, electronic, and psychological warfare into an operational command at strategic, campaign, and tactical levels. Before reforms, the national-level or strategic information operations group would have drawn units from the General Staff Department, General Political Department, and the General Armaments Department. The SSF reflects an attempt to knock down prior silos between these units and incorporating them into a cohesive force in peacetime, both to smooth over the transition to wartime, and to construct a more effective war-fighting force.

The information operations group as displayed in this parade resolves a few remaining questions on the relationship between the SSF and China's wartime structure for information operations. First and foremost, the parade formally identifies the SSF's role as the primary fighting force for information operations and "information support" (信息支援), which involves support for intelligence, surveillance, and reconnaissance in space, cyberspace, and the electromagnetic spectrum. Similar to the relationship between the other services and their corresponding operations groups, the SSF serves as the central component of the information operations group. Secondly, while the SSF is the primary fighting force for information operations, it is not the only one. Beyond the SSF, there are units from former military regions and within services that will fall under the new joint theater commands (战区) and focus on campaign-level operations. For instance, in the parade, the electronic countermeasures (ECM) formation came from the PLA, specifically from an air defense brigade and an Army Division ECM detachment (分队).<sup>[43]</sup> According to relatively authoritative literature on this concept, in a conflict scenario, each service's and branch's information countermeasures forces would combine with the information combat group (信息战斗群).<sup>[44]</sup> What is still unclear are the composition of different-echelon information operations groups, and whether tactical or campaign-level groups could have a national mission or how they would coordinate or de-conflict their respective missions.

### ***Remaining Challenges***

Thus far, in the course of PLA reforms, the Central Military Commission has focused on making broad strokes and affecting change in larger, leading organizations first, in what has been characterized as "above the neck" (脖子以上) reforms.<sup>[45]</sup> Such an approach minimizes the disruptiveness of these reforms and helps to generate buy-in from leadership on deeper cuts that will undoubtedly take place in the future. These initial steps seek to create a foundation upon which future reforms can be built. For the SSF, this has meant that the old siloed nature of space, cyber, and electronic warfare have been broken and reorganized into new verticals through the Space Systems Department and the Network Systems Department.

Such high-level changes alone, however, will not be enough to enable more profound reform. Although the SSF's force structure reflects significant progress towards a domain-

centric approach to war-fighting in the space, cyber, and electromagnetic domains, with the integration of disciplines of reconnaissance and offense, some incongruences remain at lower levels. At present, elements of the former General Staff Department's cyber, space, and electronic warfare capabilities likely remain integrated within units responsible for other missions. To follow through fully on the conceptual framework associated with the creation of the SSF, deeper, more painful cuts will need to happen to break apart and recombine existing units.

The PLA is currently engaging in “below the neck” (脖子以下) reforms, likely to be implemented over the remaining three year period through 2020 within which the reforms are intended to take place. This current stage of the process will presumably entail undertaking deeper, more difficult changes than previous changes have presaged. For the SSF, this process will test whether the PLA can fully implement the concepts and guiding paradigms that will enable better war-fighting or institutional barriers and vested interests will win the day. At this point, it remains to be seen how the SSF will make these deeper changes to restructure or otherwise integrate disparate organizational components. According to one article, in the SSF's current “grassroots construction” process, “cross-unit forces transfer and handover are progressing smoothly; new adjustment and formation of units are being completed and delimited according to plan; the system of systems architecture and contours of new-type combat forces is starting to appear...”<sup>[46]</sup> It appears that deeper changes are occurring within the SSF, with the restructuring and reorganization of units, and their transfer to different locations. The SSF's future trajectory will be a critical bellwether of the PLA's capability to implement historical organizational reforms. Indeed, its ability to function as a cohesive force would require deeper, structural changes to ensure the integration and coordination of capabilities that were previously stove-piped, perhaps in the face of considerable bureaucratic resistance.

### ***The Future of Chinese Information Operations***

The SSF will undoubtedly take on a central role as the information warfare component of China's military strategy, acting as the ‘tip of the spear’ in its strategic planning and posture. In their entirety, the PLA's military reforms seek to synthesize military preparations into an “integrated peacetime and wartime” military footing.<sup>[47]</sup> The use of “strategic presets” is intended to place China's military into an advantageous position at the outset of war, enabling it to launch a preemptive attack or quickly respond to aggression, contributing towards a first strike (先发制人) that is consistent with the perceived offense dominance of the domain.<sup>[48]</sup> This allows China to offset its disadvantages in technology and equipment through preparation and planning, particularly against a “powerful adversary” (强敌) with technological superiority, generally a byword for the US in PLA strategic literature. In practice, these strategic presets require careful selection of targets so that the first salvo of hard-kill and soft-kill measures can completely cripple

an enemy's operational 'system of systems,' or the ability to use information technology to conduct operations.

Within the context of a joint campaign, PLA information operations forces would be directed to obtain information superiority (信息优势), since to seize and preserve information dominance (制信息权) is considered an important prerequisite and foundation for joint operations.<sup>[49]</sup> In furtherance of the PLA's "system of systems" operational concept, information operations are recognized as critical means of striking "vital point targets" (要害目标) in an adversary's systems, while ensuring the continued functioning of one's systems.<sup>[50]</sup> From the PLA's perspective, achieving such information dominance is necessary for air and sea dominance.<sup>[51]</sup> *The Science of Military Strategy (SMS)*, an influential PLA textbook, calls for the coordinated employment of space, cyber, and electronic warfare means as strategic weapons to achieve these ends, to "paralyze enemy operational system of systems" and "sabotage the enemy's war command system of systems."<sup>[52]</sup> This includes launching space and cyberattacks against political, economic, and civilian targets as a deterrent. Thus, the SSF would be an integral aspect of the PLA's approach to any future informatized war and integrated strategic deterrence.

In its entirety, this emerging force structure for PLA information operations has seemingly been designed with concepts that have consistently occurred in authoritative PLA literature but could not previously be operationalized due to prior organizational divisions. Traditionally, there has a separation between cyber and electronic warfare and between reconnaissance and offensive capabilities, respectively stove-piped within 3PLA and 4PLA. The partial integration of these capabilities within the Network Systems Department could thus appreciably increase the efficacy of Chinese information operations. In particular, the PLA's concept of integrated network-electronic warfare (网电一体战, INEW), which dates back to the early 2000s, is now reflected in organizational realities, enabled by the potential integration of the relevant capabilities, and focus on the construction of new network-electronic countermeasures forces. In early writings, Major General Dai Qingmin (戴青民), former head of 4PLA, who formulated the concept of INEW, anticipated future information operations involving "the destruction and control of the enemy's information infrastructure and strategic life blood, selecting key enemy targets, and launching effective network-electronic attacks."<sup>[53]</sup> He argued that this integration of cyber and electronic warfare would be superior to the US military's approach at the time of network-centric warfare.<sup>[54]</sup>

Through its integration of space, cyber, and electronic warfare capabilities, the SSF may be uniquely able to take advantage of cross-domain synergies resulting from the inherent interrelatedness and technological convergence of operations in these domains.<sup>[55]</sup> Potentially, the Network Systems Department could thus enable the SSF to develop the capability to 'bridge the air gap' and deliver cyberattacks via electronic warfare against isolated

US battlefield networks.<sup>[56]</sup> Concurrently, the SSF's apparent responsibility for psychological warfare could enable the PLA to exploit the impactful nexus of cyber and psychological warfare capabilities, learning from the success of Russia's efforts. At this point, it is too early to evaluate whether the integrated approach to these domains and the associated disciplines that the SSF represents will be realized in practice, given the likely organizational frictions and resistance associated with such massive reforms. However, the Strategic Support Force, and the military reforms more generally, represent a new era of Chinese information operations, in which long-dormant organizational and operational concepts have found new footing in a new military order. 🇨🇳



## NOTES

1. This piece is informed by and draws upon the authors' prior writings on the SSF, which include the following: John Costello, "The Strategic Support Force: China's Information Warfare Service," *China Brief*, February 8, 2016, <https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/>. John Costello, "The Strategic Support Force: Update and Overview," *China Brief*, December 21, 2016, <https://jamestown.org/program/strategic-support-force-update-overview/>. Elsa Kania, "China's Strategic Support Force: A Force for Innovation?" *The Diplomat*, February 18, 2017, <http://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/>. Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat*, April 1, 2017, <http://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/>.
2. The authors relied upon a range of Chinese language open sources available online for this analysis. These included but were not limited to official reporting in PLA media, the publications of SSF affiliates, social media postings, and procurement notices. The authors' knowledge of Military Unit Cover Designations (MUCDs) and the names of relevant individuals were also integral to this analytical effort. Further details about sources and methods are available upon request.
3. For an expansive discussion of this concept, see: Zhou Bisong [周碧松], *Strategic Frontiers* [战略边疆], National Defense University Press [国防大学出版社], 2016.
4. Kevin McCauley, "System of Systems Operations: Enabling Joint Operations," Jamestown Foundation, February 28, 2017, <https://jamestown.org/product/pla-system-systems-operations-enabling-joint-operations-kevin-mccauley/>. Joel Wunthrow, "A Brave New World for Chinese Joint Operations," *Journal of Strategic Studies*, Volume 40, 2017, <http://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1276012?journalCode=fjss20>.
5. James C Mulvenon, "The PLA and Information Warfare," *In The People's Liberation Army in the Information Age*, Vol. 145, Rand Corporation, 1999.
6. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-aptl-report.pdf>.
7. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Department of Justice: Office of Public Affairs, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.
8. "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," September 25, 2015, The White House Office of the Press Secretary, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.
9. FireEye iSight Intelligence, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," June 20, 2016, <https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html>.
10. Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," May 17, 2017, <https://www.recordedfuture.com/chinese-mss-behind-apt3/>.
11. "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," Department of Justice Office of Public Affairs, November 27, 2017, <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>.
12. Jack Goldsmith and Robert D. Williams, "The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage," *Lawfare*, November 30, 2017, <https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage>.
13. Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers, "China's Cybersecurity Law One Year on", *DigiChina*, November 30, 2017, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>.
14. Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press [国防大学出版社], 2015.
15. For a more detailed analysis of these reforms, see: Joel Wunthnow and Phillip C. Saunders, "Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications," *China Strategic Perspectives*: NDU Press, March 2017, <http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf?ver=2017-03-21-152018-430>.
16. *Strategic Frontiers* [战略边疆], China Strategic Support, August 15, 2016, [http://zlzy.81.cn/tb/2016-08/15/content\\_7231775.htm](http://zlzy.81.cn/tb/2016-08/15/content_7231775.htm).



## NOTES

17. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (eds.), *The Science of Military Strategy* [战略学].
18. “All Military Actual Combat Military Training Forum Delegates Deliver a Speech” [全军实战化军事训练座谈会代表发言摘登], *PLA Daily*, August 7, 2016, <http://military.people.com.cn/nl/2016/0807/c1011-28616977.html>.
19. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed). *The Science of Military Strategy* [战略学], Military Science Press, 2013.
20. Liu Wei (刘伟) (ed.), *Theater Command Joint Operations Command* (战区联合作战指挥), National Defense University Press (国防大学出版社), 2016.
21. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds. *The Science of Military Strategy* [战略学]. Military Science Press [军事科学出版社], 2013.
22. Xiao Tianliang [肖天亮] (eds.), *The Science of Military Strategy* [战略学], National Defense University Press [国防大学出版社], 2015, 388.
23. “Reshape Cyberspace Military-Civil Fusion Talent Cultivation” [重塑网络空间军民融合人才培养], *People’s Daily Online*, September 15, 2017, <http://media.people.com.cn/nl/2017/0915/c414363-29538892.html>.
24. “The SSF and 9 Local Units Cooperate to Cultivate High-Level Talent for New-Type Forces” [战略支援部队与地方9个单位合作培养新型作战力量高端人才], *Xinhua*, July 12, 2017, [http://news.xinhuanet.com/politics/2017-07/12/c\\_1121308932.htm](http://news.xinhuanet.com/politics/2017-07/12/c_1121308932.htm).
25. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学]. Military Science Press [军事科学出版社], 2013.
26. Ye Zheng [叶征]. A Discussion of the Innate Characteristics, the Composition of Forces, and the Included Forms” [论网络空间战略博弈的本质特征, 力量构成与内容形势], *China Information Security* [中国信息安全], August 2014.
27. Gao Jin’s role as commander of the SSF is noteworthy in two respects: First, he is a career Second Artillery officer, so his new role muddies the waters a bit in understanding whether the SSF will be a force composed of Army personnel but treated administratively separate from the Army—not unlike the former PLASAF-PLA Army relationship—or will be composed of personnel from various services and treated administratively separate from all forces. Secondly and more important to this discussion, before his new post as SSF commander, Gao Jin was head of the highly-influential Academy of Military Sciences (AMS) which besides being the PLA’s think-tank (along with the National Defense University), is responsible for putting out *The Science of Military Strategy*, a wide-reaching consensus text that captures and guides PLA strategic thinking at the national level. The most recent edition published in 2013 was released under his tenure as commandant of AMS, and many of the ideas from that edition have found their way into the 2015 defense white paper and have informed the reform agenda. His new role could thus be seen as CMC-level endorsement of the views on China’s strategic thought contained in *The Science of Military Strategy*.
28. See, for instance: “Gao Jin Becomes Strategic Support Force Commander” [高津任战略支援部队司令员], *Sina*, January 1, 2016, <http://news.sina.com.cn/c/sz/2016-01-01/doc-ixfnept3519173.shtml>.
29. There is a growing number of public records that link former 3PLA units and facilities—including former Technical Reconnaissance Bureaus and the 3PLA headquarters itself—to the SSF.
30. The sources are available upon request.
31. Several open sources all indicate their transfer to the SSF.
32. See, for instance, Mark Stokes, Russell Hsiao, and Jenny Lin, “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” Project 2049, November 11, 2011, [https://project2049.net/documents/pla\\_third\\_department\\_sigint\\_cyber\\_stokes\\_lin\\_hsiao.pdf](https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf).
33. The 56th Research Institute focuses on research and development of advanced computing technologies, including supercomputers. The 57th Research Institute seems to engage the development of communications intercept and signal processing systems, and it has also focused on satellite communications technology. The 58th RI focuses on cryptography and information security.

## NOTES

34. Several open sources indicate this transfer, including: “How Can the Strategic Support Force Forge New Quality Weapons” [战略支援部队如何锻造新质利器], *PLA Daily*, March 11, 2016, <http://www.chinanews.com/mil/2016/03-11/7792939.shtml>.
35. Wang Jinsong (王劲松), Wang Nanxing (王南星), and Ha Junxian (哈军贤), “Research on Cyberspace Operations Command” [网络空间作战指挥研究], *Journey of the Academy of Armored Force Engineering* [装甲兵工程学院学报], October 2016.
36. “After a Year of Military Reform, Reviewing “New Institution Time” in the Military Newspaper’s Published Articles” [军改一周年 军报刊文回眸“新体制时间”之变], *PLA Daily*, December 2, 2016, <http://military.people.com.cn/n1/2016/1202/cl011-28919716.html>.
37. The relevant sources are available upon request.
38. The relevant sources are available upon request.
39. Wang Jinsong (王劲松), Wang Nanxing (王南星), and Ha Junxian (哈军贤), “Research on Cyberspace Operations Command” [网络空间作战指挥研究], *Journal of the Academy of Armored Force Engineering* [装甲兵工程学院学报], October 2016.
40. *Lectures on the Command of Joint Campaigns* [联合战役指挥教程], Military Science Press, 2013, 218-222.
41. Dennis J. Blasko, Elsa B. Kania, and John K. Costello, “The PLA at 90: On the Road to Becoming a World-Class Military?,” *China Brief*, August 10, 2017.
42. Ibid. For a full listing of formations in the parade see: *PLA Daily*, August 1, [http://www.81.cn/jfjbmap/content/2017-08/01/content\\_183726.htm](http://www.81.cn/jfjbmap/content/2017-08/01/content_183726.htm) and related official media coverage.
43. “The Electronic Countermeasures Formation” (电子对抗方队), *Xinhua*, July 30, 2017, [http://news.xinhuanet.com/politics/2017-07/30/c\\_1121402312.htm](http://news.xinhuanet.com/politics/2017-07/30/c_1121402312.htm).
44. *Science of Joint Tactics* [联合战术学], Military Science Press, 2013, 120.
45. “‘Below the Neck’ Reforms Begin” [“脖子以下”改革展开], *China Military Online*, December 19, 2016, [http://www.81.cn/jmywyl/2016-12/19/content\\_7413070\\_2.htm](http://www.81.cn/jmywyl/2016-12/19/content_7413070_2.htm).
46. “Exposition on Strategic Support Force Grassroots Construction” [战略支援部队基层建设工作述评], September 24, 2017, <http://military.worker.cn/268/201709/24/170924102952875.shtml>.
47. Liu Wei (刘伟) (ed.), *Theater Command Joint Operations Command* (战区联合作战指挥), National Defense University Press (国防大学出版社), 2016.
48. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed.), *The Science of Military Strategy* [战略学], 320.
49. *Lectures on the Command of Joint Campaigns* [联合战役指挥教程], Military Science Press, 2013, 218-222.
50. Ibid.
51. Ibid, 165.
52. Ibid, 164.
53. Dai Qingmin, “On Seizing Information Supremacy,” *Zhongguo Junshi Kexue*, April 20, 2003. qtd. in Larry M. Wortzel, “The Chinese People’s Liberation Army and Information Warfare,” *Strategic Studies Institute*, March 2014.
54. Dai Qingmin [戴清民]. *A New Perspective on Warfare* [战争新视点], Liberation Army Press [解放军出版社], 2008.
55. John Costello, “Bridging the Air Gap: The Coming Third Offset,” February 17, 2015, *War on the Rocks*, <https://warontherocks.com/2015/02/bridging-the-air-gap-the-coming-third-offset/>.
56. Ibid.



# Determinants of the Cyber Escalation Ladder

---

Nadiya Kostyuk

Scott Powell

Matt Skach

## ABSTRACT

**T**his article investigates how the speed and sophistication of cyber tools shape modern conflict. Using the United States as a case study, it looks at how, when, and why physical and cyber affronts can quickly escalate, and what appropriate counter-actions exist at each stage of the conflict. We also briefly contrast the US physical and cyber conflict escalation ladders with those of China and Russia. Our work has important implications for policy-makers and military leaders as it demonstrates the importance of having cyber escalation ladders for each country. We stress that not only should these ladders include country-specific perceptions of various actors and their likely motivations, but they should also account for other actors' differences in perception of various physical and cyber actions. The latter could lead to a difference in each state's understanding of the others' escalation ladders, and thus unexpected responses.

**Keywords:** *cyber escalation ladders, cyber conflict, spectrum of conflict, the US, China, Russia*

The first known cyberattack to cause an electrical power outage occurred in Ukraine at the end of 2015.<sup>[1]</sup> On December 23rd, hackers disabled control systems used to coordinate remote substations, leaving people in Kyiv, the capital of Ukraine, and the western part of the country without power for several hours. A year later, presumably the same group of hackers attacked the power grid in Kyiv. The Security Service of Ukraine blamed the Russian government for both nefarious acts.<sup>[2]</sup> The computer security firm *iSight Partners* attributed these hacks to Sandworm; a group believed to have Russia origins.<sup>[3]</sup> Because of inferior cyber capabilities, the Ukrainian government decided not to retaliate but to verbally condemn the Russian government for this act of *cyber warfare*.<sup>[4]</sup> If Sandworm, representing the Russian government, had faced a better-equipped opponent, the cyber events could have quickly escalated in virtual and, potentially, physical fronts.

© 2017 Nadiya Kostyuk, Scott Powell, Matt Skach



Nadiya Kostyuk is a Fellow for the Cybersecurity Project at the Belfer Center and is completing her PhD at the University of Michigan in Political Science and Public Policy. She is also a research fellow at the Cybersecurity, Internet Governance, Digital Economy, and Civic Tech Initiative at Columbia's School of International and Public Affairs during the 2017-2018 academic year. Nadiya's research interests are states' cyber capacities; cyberattacks as coercive tools; mapping physical and 'digital' fronts. Her regional expertise includes post-Soviet countries. She is currently a fellow at EastWest Institute of Global Cooperation in Cyberspace Initiative.

### *Spectrum of Conflict*

We use the Spectrum of Conflict ("the Spectrum", thereafter) as defined in the 2008 Army Field Manual 3-0, Operations<sup>[5]</sup> ("The Manual", thereafter), to outline the Spectrum of Conflict for conventional and cyber actions. The manual divides the Spectrum of conflict into stable peace, unstable peace, insurgency, and general war.<sup>[6]</sup> At each stage, the US, its allies, and its adversaries—state or non-state actors—have various cyber tools available. Additionally, motivations for these actions vary as widely as the tools and types of actors that employ them.<sup>[7]</sup> Having determined potential suspects of cyberattacks and their possible motive, an actor should decide where to place the committed cyber misbehavior in the Spectrum, as well as where the other side similarly perceives such action on their Spectrum.<sup>[8]</sup> For instance, a hostile actor may conduct espionage during stable peace, but could also conduct the same activity during insurgency or unstable peace. Depending on these perceptions, state and non-state actor responses may vary.

### *Escalation Ladder*

When deciding the appropriate response to a cyberattack, the US should account for the following factors. *First, who is the attacker, and what is their objective?* For instance, industrial espionage may not require a declaration of war, but sabotage of the power grid may require more than a denial of service attack. *Second, where does the US consider itself in the Spectrum?* If it is in unstable peace, diplomatic actions or brandishing capabilities may prove to be useful deterrents. When conducting an exercise to brandish capabilities, the US should determine if exposing a capability is useful and what end-state is it trying to achieve—making an adversary look powerless or the US to appear powerful.<sup>[9]</sup> Finally, *second-order effects are worth*



Scott Powell is a former Army officer and 2005 graduate of the United States Military Academy. He is also a recent graduate of the Gerald R. Ford School of Public Policy.

*considering*; these effects can include unintended damage, whether physical or otherwise, and the possibility of further escalation by an adversary.

In this section, we build a cyber escalation ladder (Table 1) aligning the Spectrum of Conflict, a proposed escalation ladder, and the types of kinetic (non-cyber) and cyberattacks that may emerge at each level.

### ***Building the Ladder***

The Spectrum of Conflict's lowest rung is a stable peace. In this preparatory phase, cyber activity is directed towards developing the capability to offensive and defensive cyber actions. This means that effective cyber forces, even with no immediate threat on the horizon, must continuously build and maintain its cyber capabilities by recruiting, training and organizing cyber forces as well as providing them with the financial, technological, organizational, and infrastructure resources needed for their mission. In addition, these forces should develop contingency plans and be ready to defend against threats in cyberspace that appear with little or no advanced warning. These conditions are needed in preparation for an adversary taking hostile actions towards unstable peace or any other form of escalation.

In a conflict that escalates into minor harassment, cyber activities expand to exploit weaknesses in an adversary's system without disrupting operations or damage infrastructure. The mission of the US cyber forces at this Spectrum level incorporates all of the prior actions and expands to include espionage and cyber counterintelligence, gathering credentials, and propaganda. Credential collection is an important activity to launch larger scale cyberattacks or facilitate the access of information on protected systems.<sup>[10]</sup> As intelligence gathering is an accepted norm, it should not be considered escalatory.



Matt Skach is a PhD candidate in the Department of Computer Science and Engineering at the University of Michigan, and a combat engineer in the 1433rd Engineering Company of the Michigan Army National Guard. His research interests include novel design and technologies for large-scale computer systems and data centers. Skach has an MS in electrical engineering from the University of Michigan and a BS in electrical engineering from Oregon State University.

Propaganda, although not explicitly a cyber-attack, can incorporate cyber elements to enhance the spread or impact of a message. In response to the early conflict in Ukraine, social media emerged as a major channel of communication for protesters and international observers, and Russia utilized the “comments” section of news sites to promote pro-Russian dialogue on domestic and foreign websites.<sup>[11]</sup> In a more direct approach that may cross the border into unstable peace occurred during the 2016 US Presidential Election. Russia combined an extensive propaganda campaign with cyber-attacks on the Democratic National Committee and subsequent release of damaging emails through WikiLeaks in an attempt to influence the outcome.<sup>[12]</sup>

Moving upwards from stable peace to an unstable peace, cyber activities at the major harassment level aggressively exploit weaknesses and disrupt daily operations, but do not cause permanent damage to infrastructure or compromise systems. On the conventional (non-cyber) side, sanctions are a common tool used by the US and exemplified by their reaction to Russian interference in the 2016 Presidential election.<sup>[13]</sup> At this stage, equivalent cyber operations include overt demonstrations of cyber capability to deter the opponent and minor denial of service (DOS) attacks that exert influence but do little permanent damage. Overt displays of cyber capability such as the defacement of public websites were a common tool of the hacktivist group Anonymous during Operation China in response to China’s crackdown on protests.<sup>[13]</sup> Similarly, DOS attacks that deny cyber or non-cyber infrastructure can pose varying levels of inconvenience against an adversary. Lizard Squad, a hacktivist group, launched distributed denial of service (DDOS) attacks against Sony’s PlayStation Network and Microsoft’s Xbox Live services.<sup>[15]</sup> Website defacement



and DDOS by an adversary can present a significant inconvenience but poses little risk of permanent damage.

Although initiated in cyberspace, the impact of DOS and DDOS attacks are not limited to the cyber domain. ‘SWATing’<sup>[16]</sup> and other attacks that focus on emergency services, if applied on a large scale, could be used to tie up law enforcement resources and other emergency first responders (EFR). SWATing style attacks pose an increased risk of injury or loss of life over DOS cyberattacks, but neither of these incursions alone is likely to be escalatory.

Moving up the escalation ladder from harassment to minor damaging attacks, cyberspace enables a range of low-financial-cost attacks that compromise non-critical data or inflict minor, repairable damage. Potential targets include the destruction of non-critical data on networked systems and the targeted harassment of military infrastructure. Sony Pictures suffered a massive data loss in 2014 at the hands of North Korean state hackers,<sup>[17]</sup> and Saudi Aramco lost data on 35,000 hard drives in a 2012 cyberattack.<sup>[18]</sup> The attacks did not pose a significant disruption of services outside of the affected company, and neither event prompted retaliation, but both companies faced severe financial costs to restore services. On the other hand, WannaCrypt,<sup>[19]</sup> one of the most significant Ransomware attacks to date, demonstrated the compelling capability to tie up businesses and critical services such as hospitals by encrypting data and holding it ransom until demands are met. There exists the potential for extensive collateral damage from this type of cyberattack. This is fundamentally different from traditional DOS attacks that temporarily make a site or service inaccessible, as opposed to Ransomware that may permanently destroy data if demands are not met.

Although WannaCrypt primarily struck unpatched civilian targets, there is the potential for targeted harassment of military infrastructure. Interference actions that target non-critical military services stand to interrupt day-to-day operations by delaying email communication or hindering logistics, but do not pose a significant threat to critical military infrastructures such as strategic missile or air defense systems. Similarly, interference or delay of supplies can pose a problem, but outside of a war zone, it is unlikely to pose a critical threat to combat readiness. Highly targeted attacks with limited destructive capability such as Stuxnet<sup>[20]</sup> may also be deployed at this level. These attacks are not inherently escalatory, but depending on the target and duration of the attack the risk posed by the vulnerability may be considered escalatory (e.g., hindering communications may be seen as the prelude to a larger attack). Smaller cyberattacks may also become escalatory when paired with other kinetic attacks. A DOS attack on EFR services combined with a limited kinetic action such as a drone strike could increase the net effect from a minor damaging attack to a major one when EFR resources are not immediately available to treat casualties.



Continuing to escalate from minor to major damaging attacks, where conventional kinetic attacks come into play, cyberattacks escalate to include compromising critical data and causing damage to systems or infrastructure that is not quickly repaired and degrades military capabilities. Both kinetic and cyberattacks at this level are designed to disable or destroy critical military infrastructure; disabling early warning systems, as well as targeted instruction or information dispersal. In an early example of cyber warfare, the Israeli military subverted and disabled Syrian air defenses before conducting an aerial strike on a Syrian nuclear facility.<sup>[21]</sup> The US military also proposed but ultimately decided against an attempt to disable Iraqi air defenses through a cyberattack before the 2003 invasion.<sup>[22]</sup> The US did, however, email instructions to Iraqi military officers using Iraq's email system on how they should surrender to Coalition forces before the ground invasion.<sup>[23]</sup> These and larger cyberattacks should be considered escalatory in nature.

Beyond major damaging attacks lie catastrophic and existential attacks. A catastrophic cyberattack is one that compromises national security and requires a response so massive it would prevent the US from addressing other contingencies for the duration of the conflict. Existential attacks are those that would potentially result in the destruction of the US or collapse of its society, for example, a bilateral nuclear war.

Permanent damage to civilian infrastructure such as power and utility grids has the potential to become a catastrophic attack affecting millions of people. At present, we do not believe a single mode of cyberattack alone would pose an existential threat to the US, however, this may change in the near future. Although many (if not most) utility grids are currently connected to the Internet, they are segregated regionally by hundreds of local companies that reduce the potential impact of a widespread outage. However, in addition to critical utility grids, food production and logistics are rapidly becoming automated and connected to the Internet.<sup>[24]</sup> A large-scale, long-lasting attack on the food production or supply distribution network once manual systems are sufficiently scarce could create devastating casualties comparable to a small-scale nuclear strike.

### ***The Ladder***

In Table 1, we assemble the Spectrum of Conflict and associated actions at each level into a single ladder. The first column contains the Spectrum of Conflict, from Stable Peace to General War, and the second column includes levels of damage from No Activity up through Catastrophic Attacks. Column 3 lists potential actions and responses using non-cyber options, and column 4 provides examples of cyberattacks that align with the options from column 3. As some rungs of the ladder or types of attacks may occur in more than one category, the boxes from one column may overlap boxes from another column to indicate the different levels of possible actions and consequences.

Spectrum of Conflict	Escalation Ladder	Conventional Actions	Cyber Actions
	Preparation	<ul style="list-style-type: none"> <li>Training</li> <li>Infrastructure development</li> <li>Implement SOPs</li> </ul>	<ul style="list-style-type: none"> <li>Recruit, train, organize hackers</li> <li>Develop plans</li> <li>Cyber defense, counter espionage</li> </ul>
	Minor Harassment	<ul style="list-style-type: none"> <li>Diplomatic protest</li> <li>Legal action</li> <li>Espionage</li> </ul>	<ul style="list-style-type: none"> <li>Public influence, propaganda</li> <li>Cyber espionage, cyber counterintelligence</li> <li>Gathering credentials</li> </ul>
UNSTABLE PEACE	Major Harassment	<ul style="list-style-type: none"> <li>Economic sanctions</li> </ul>	<ul style="list-style-type: none"> <li>Overt demonstration of cyber capability</li> <li>Inconveniencing attacks (DOS embassies &amp; minor services, SWATing, tie up EFR resources)</li> </ul>
	Minor Damaging Attacks	<ul style="list-style-type: none"> <li>Limited kinetic attacks (raids, drone strikes)</li> </ul>	<ul style="list-style-type: none"> <li>Destruction of non-critical data</li> <li>Targeted harassment of military infrastructure (DOS, logistics interference)</li> </ul>
INSURGENCY	Major Damaging Attacks	<ul style="list-style-type: none"> <li>Limited contingency operations<sup>25</sup></li> </ul>	<ul style="list-style-type: none"> <li>Targeted military interference</li> <li>Overt targeted disabling and/or destruction of military targets or infrastructure</li> </ul>
		<ul style="list-style-type: none"> <li>Major military operations (invasion, regime change)</li> </ul>	
GENERAL WAR	Catastrophic Attacks	<ul style="list-style-type: none"> <li>Nuclear War</li> </ul>	<ul style="list-style-type: none"> <li>Permanent damage to civilian infrastructure (mass destruction of critical data, infrastructure control software, banking infrastructure)</li> </ul>
	Existential Attack		<ul style="list-style-type: none"> <li>Nothing (yet)</li> </ul>

Table 1: Escalation Ladder


### *Differences in Perceptions Leading to Potential Escalation*

Potential adversaries such as Russia and China have similar views on the escalation ladder when it comes to the online environment, but some important differences do exist. Besides the most commonly used cyber tools, such as espionage,<sup>[26]</sup> DDOS and spear-phishing, both countries give a high priority to their information space. Harmony in society is vital for China and Russia, and inciting anti-government propaganda, for instance, might be considered an existential threat.

China's Internet is subject to the control of the Ministry of Public Security.<sup>[27]</sup> Also, the government uses computer specialists for managing its domestic blogosphere.<sup>[28]</sup> The government tries to create an impression of freedom of speech by planting people in online debates to influence public opinion.<sup>[29]</sup> One goal of the state is to shield its Internet users from outside influences—mainly from Western countries—aiming to block such issues such as “human rights, democracy, and religion.”<sup>[30]</sup> Besides being protected by the Great Firewall, the Chinese People's Liberation Army (PLA) remain alert in case such a threat from the West arises.

Such concern is widely shared by Russia, whose greatest fear is “circulation of [uncontrolled and Western-influenced] information.”<sup>[31]</sup> Western cybersecurity experts believe Russia is afraid that its entire population could serve as the target of influence for an enemy disinformation campaign.<sup>[32]</sup> This concern is even documented in the country's laws<sup>[33]</sup> that outline the circumstances in which Russia would deploy its armed forces in the territory of other states to provide information security.<sup>[34]</sup> Even a minor violation of such harmony in the society supported by the control of information can quickly lead to escalation on the cyber action ladder. Creating Russia's and China's escalation ladders is a crucial step for future research on this topic.

## **CONCLUSION**

By 2020, on average, each American will have five internet-connected devices that bring various vulnerabilities that are readily exploitable during a conflict. States should be aware of each other's position on physical and escalation ladders before engaging in a cyber conflict. Using the US as a case study, we demonstrated the challenges that nation-states face when forming appropriate responses to US cyber actions. These challenges also apply to other state actors. Not only should they decide who the attackers are and their likely motivations, but they should account for other actors' differences in perception of various actions. The latter could lead to a difference in each state's understanding of the other's escalation ladder, and unexpected responses. Therefore, it is important to understand what norms each state associates with various attacks, and what it may infer about the attacker's intentions since “in cyberspace as in other realms of warfare, ‘the defender frequently does not understand how threatening his behavior, though defensively motivated, may seem to the other side.’”<sup>[35]</sup> 

### *Acknowledgements*

We would like to thank the CDR reviewers and editors for their helpful comments and feedback. We would also like to thank Professor Robert Axelrod of the Gerald R. Ford School of Public Policy at the University of Michigan for his guidance and input. Company and product names within this publication are used for identification purposes and may be trademarks of their respective owners.

## NOTES

1. Ellen Nakashima, “Russian hackers suspected in attack that blacked out parts of Ukraine,” *The Washington Post*, January 5, 2016.
2. Kim Zetter, “Everything we know about Ukraine’s power plant hack,” *Wired*, January 20, 2016.
3. *Ibid*.
4. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).
5. Even though FM 3-0 is now ADP/ADRP 3-0 with an update in 2016, we decided to use the older version of the document FM 3-0, as the new one does not have a spectrum of conflict in it. Despite the fact that we are using the older version, our main argument does not change.
6. Department of the Army, “FM 3-0 C-1”, February 2008. This manual defines *stable peace* as “an operational environment characterized by the absence of militarily significant violence.” The manual defines *unstable peace* as the conditions “when one or more parties threaten or use violence to accomplish their objectives, stable peace degenerates into *unstable peace*. Unstable peace may also result when violence levels decrease after violent conflict.” The manual defines *insurgency* as “the organized movement of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority.” The manual defines *general war* as the conditions when “armed conflict between major powers in which the belligerents have used all their resources, and the national survival of a major belligerent is in jeopardy. Diplomatic and economic channels have broken down.”
7. Some potential motivations may include money, espionage, skills for employment, fame, entertainment, hacktivism, terrorism, or war. From: Jason Andress and Steve Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners* (Elsevier, 2013), 48.
8. Differences in perception will be discussed in the later section.
9. Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Rand Corporation, 2013), vii-xi.
10. Kim Zetter, “NSA Hacker Chief Explains How to Keep Him Out of Your System,” *Wired*, January 20, 2016.
11. Shaun Walker, “Salutin’ Putin: inside a Russian troll house,” *The Guardian*, April 2, 2015; David Stern, “The Twitter War: Social Media’s Role in Ukraine Unrest,” *National Geographic*, May 11, 2014.
12. “U.S. Intelligence Report Identifies Russians Who Gave DNC Emails to Wikileaks,” *Time*, January 5, 2017.
13. David Sanger, “Obama Strikes Back at Russia for Election Hacking,” *The New York Times*, December 29, 2016.
14. Mary-Ann Russon, “Anonymous brings down 30 Chinese government websites to support Hong Kong protestors,” *International Business Times*, April 13, 2015.
15. Dylan Love, “Why Microsoft and Sony couldn’t stop Lizard Squad attack despite warnings,” *International Business Times*, December 30, 2014.
16. Federal Bureau of Investigation, “The Crime of ‘Swatting,’” September 12, 2013.
17. Peter Elkind, “Sony hack,” *Fortune Magazine*, July 1, 2015.
18. Jose Pagliery, “The inside story of the biggest hack in history,” *CNN*, August 5, 2015.
19. David Sanger, Sewell Chan and Mark Scott, “Ransomware’s Aftershocks Feared as U.S. Warns of Complexity,” *The New York Times*, May 14, 2017.
20. Kim Zetter, “How digital detectives deciphered STUXNET, the most menacing malware in history,” *Wired*, August 11, 2011.
21. Richard Alan Clarke and Robert K. Knake, *Cyber War* (Harper-Collins, 2010), 1-9.
22. *Ibid*.
23. *Ibid*, 9-11.
24. Dave Bradford, “Old McDonald had an algorithm-driven prescriptive planting service,” *Cyber Risk Network*, November 4, 2012; George Westerman, “The Internet-connected engine will change trucking,” *Harvard Business Review*, November 4, 2012.

## NOTES

25. For definitions see: Pub, Joint, “3-0. Doctrine for Joint Operations,” *Washington DC: Joint Chiefs of Staff* (1995).

26. For instance, China is famous for its cyber espionage operations (Reveron 2012); The Mandiant report highlights the peculiarities of the Chinese hacking U.S. infrastructure, government, ministries, and financial sector for over a decade with the main purpose of stealing information (Westby 2013); Derek S. Reveron, *Cyberspace and national security: threats, opportunities, and power in a virtual world* (Georgetown University Press, 2012); Jody Westby, “Mandiant report on Chinese hackers is not news but its approach is.” *Forbes Magazine*, February 20, 2013.

27. Derek S. Reveron, *Cyberspace and national security: threats, opportunities, and power in a virtual world* (Georgetown University Press, 2012).

28. *Ibid*

29. *Ibid*

30. Nigel Inkster, “China in cyberspace,” *Survival* 52, no. 4 (2010), 55-66.

31. Kerstin Pertermann, *Challenges in cybersecurity: risks, strategies, and confidence-building; international conference* (Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, 2012).

32. “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space,” Section 1, Fundamental Terms and Definitions, *The Russian Federation* (NATO Cooperative Cyber Defense Centre of Excellence, 2011); Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Foreign Military Studies Office, 2011).

33. These laws include: the 2000 Doctrine of the Information Security of the Russian Federation (RF) and the 2011 “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space.”

34. Keir Giles, “Russia’s public stance on cyberspace issues,” (IEEE: Cyber Conflict (CYCON), 2012 4th International Conference, 2012), 1-13.

35. Barry R. Posen, “Inadvertent Nuclear War? Escalation and NATO’s Northern Flank,” *International Security* 7, no. 2 (1982), 28-54.



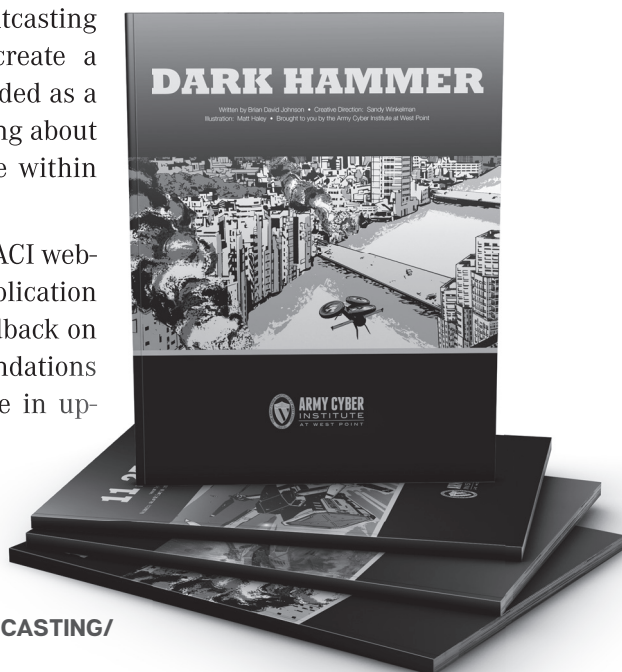


# THREATCASTING Graphic Novels

Helping the U.S. Army understand and plan for the future operating environment is at the heart of a project known as Threatcasting. Led by the Army Cyber Institute at West Point, in collaboration with Arizona State University's School for the Future of Innovation in Society, the process gives researchers a structured way to envision and plan for risks ten years in the future.

The Army has a long history of using graphic novels and fiction to help the force understand abstract topics. The future use of cyber by our military and adversaries is tailored-made for graphical storytelling. Therefore, the ACI commissioned a creative team of writers and illustrators to combine the Threatcasting findings with military expertise to create a series of graphic novels. They are intended as a conversation piece to get the force talking about cyber as it relates to their specific role within the military.

The first four graphic novels are on the ACI website with additional work slated for publication this year. We are interested in your feedback on the current novels, and also recommendations on 'future challenges' we should tackle in upcoming issues.



[CYBER.ARMY.MIL/WORK-AREAS/THREATCASTING/](http://CYBER.ARMY.MIL/WORK-AREAS/THREATCASTING/)



# THE CYBER DEFENSE REVIEW

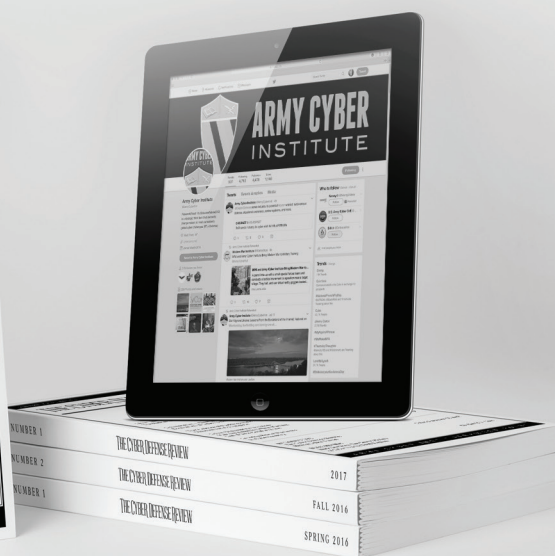
CONTINUE THE CONVERSATION ONLINE

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

AND THROUGH SOCIAL MEDIA

 Facebook @armycyberinstitute

 Twitter @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.