

THE CYBER DEFENSE REVIEW

Cybersecurity: Focusing on Readiness and Resiliency for Mission Assurance
Rear Admiral Danelle Barrett



Cyberspace Operations Collateral Damage –
Reality or Misconception?

Mr. Giorgio Bertoli
Dr. Lisa Marvel

The Cyber Domain

Dr. Glenn Alexander Crowther

Cyber Threat Characterization

Dr. Kamal Jabbour
Dr. Erich Devendorf

Maneuverable Applications: Advancing
Distributed Computing

Dr. William Clay Moody
Dr. Amy Apon

Digital Network Resilience: Surprising
Lessons from the Maginot Line

Mr. Ray Rothrock

INTRODUCTION

The Cyber Defense Review:
Continuing our Interdisciplinary Journey

Colonel Andrew O. Hall

BOOK REVIEW

*Data and Goliath: The Hidden Battles to
Collect Your Data and Control Your World*
by Bruce Schneier

Dr. Jan Kallberg
Cadet Monte Ho

THE CYBER DEFENSE REVIEW

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

EDITOR IN CHIEF

Corvin J. Connolly, Ph.D.

MANAGING EDITOR

Jan Kallberg, Ph.D.

ASSISTANT EDITORS

Harold Arata, Ph.D.

Aaron F. Brantly, Ph.D.

Paul Goethals, Ph.D., Col. (U.S. Army)

Michael Grimaila, Ph.D.

Charlie Lewis, Maj. (U.S. Army)

Martin Libicki, Ph.D.

Fernando Maymi, Ph.D.

Jeffrey Morris, Ph.D., M.Sgt. (U.S. Army)

Paulo Shakarian, Ph.D.

David Thomson, Ph.D.

Robert Thomson, Ph.D.

Natalie Vanatta, Ph.D., Maj. (U.S. Army)

ADVISORY BOARD

Andrew O. Hall, Ph.D., Col. (U.S. Army) – Chair.

Chris Arney, Ph.D., Brig. Gen. (U.S. Army Ret.)

Daniel Bennett, Ph.D., Col. (U.S. Army)

Dave Branch, Col. (U.S. Army)

Donald L. Carmel, Jr., Col. (U.S. Army Ret.)

Judy Esquibel, Chief Warrant Officer 3 (U.S. Army)

Christopher Hartley (U.S. Army)

Rhett A. Hernandez, Lt. Gen. (U.S. Army Ret.)

Edward Sobiesk, Ph.D., Col. (U.S. Army Ret.)

J. Carlos Vega, Col. (U.S. Army)

CREATIVE DIRECTORS

Michelle Grierson

Gina Daschbach

LEGAL REVIEW

Courtney Gordon-Tennant, Esq.
(U.S. Army)

PUBLIC AFFAIRS OFFICER

Terence M. Kelley, Maj.
(U.S. Army)

KEY CONTRIBUTORS

Clare Blackmon

Nataliya Brantly

Erik Dean

Katherine Hutton

Kristin Kohler

Asuman Mielke

Alfred Pacenza

Irina Garrido de Stanton

CONTACT

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

SUBMISSIONS

The Cyber Defense Review welcomes submissions.

Please contact us at cyberdefensereview@usma.edu.

SUBSCRIBE

Digital: cyberdefensereview.army.mil

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

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

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

∞ Printed on Acid Free paper.

INTRODUCTION

COLONEL ANDREW O. HALL	09	<i>The Cyber Defense Review:</i> Continuing our Interdisciplinary Journey
------------------------	----	---

SENIOR LEADER PERSPECTIVE

REAR ADMIRAL DANELLE BARRETT	15	Cybersecurity: Focusing on Readiness and Resiliency for Mission Assurance
------------------------------	----	---

PROFESSIONAL COMMENTARY

T. CASEY FLEMING ERIC L. QUALKENBUSH ANTHONY M. CHAPA	25	The Secret War Against the United States
RAY A. ROTHROCK	33	Digital Network Resilience: Surprising Lessons from the Maginot Line
OZ SULTAN	41	Combatting the Rise of ISIS 2.0 and Terrorism 3.0

RESEARCH ARTICLES

GIORGIO BERTOLI DR. LISA MARVEL	53	Cyberspace Operations Collateral Damage - Reality or Misconception?
DR. GLENN ALEXANDER CROWTHER	63	The Cyber Domain
DR. KAMAL T. JABBOUR DR. ERICH DEVENDORF	79	Cyber Threat Characterization

RALPH MARTINS

95

Anonymous' Cyberwar Against
ISIS and the Asymmetrical
Nature of Cyber Conflict

**LIEUTENANT COLONEL
WILLIAM CLAY MOODY
DR. AMY W. APON**

107

Maneuverable Applications:
Advancing Distributed
Computing

RESEARCH NOTES

**DR. JAN KALLBERG
CAPTAIN W. BLAKE RHOADES
MARCUS J. MASELLO
DR. ROSEMARY A. BURK**

129

Defending the Democratic Open
Society in the Cyber Age – Open
Data as Democratic Enabler and
Attack Vector

TOM WATERS

139

Multifactor Authentication –
A New Chain of Custody Option
for Military Logistics

BOOK REVIEW

**DR. JAN KALLBERG
CADET MONTE HO**

150

*Data and Goliath: The Hidden
Battles to Collect Your Data and
Control Your World* by Bruce
Schneier

THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

The Cyber Defense Review: Continuing our Interdisciplinary Journey

Colonel Andrew O. Hall



INTRODUCTION

Welcome to our fall edition of *The Cyber Defense Review*. We have added a couple of exciting innovations with this issue and some very thought-provoking pieces. First, I am happy to announce that the *CDR* is on JSTOR, providing an impressive extension of our distribution to their worldwide network of libraries and institutions. We also have added a research notes section. These high-velocity discussion papers are targeted at time-sensitive research and run between 1,500 and 3,000 words. This innovation provides another exciting section to add to our professional commentary and peer-reviewed research articles.

This issue features senior commentary from RDML Danelle Barrett addressing cyber terrain and mission assurance, continuing a timely and important discussion for our joint force. Casey Fleming, Ray Rothrock, and Oz Sultan will take us on a tour of cyber conflict ranging from hybrid warfare to the Maginot Line and combating ISIS and terrorism on the web.

Our research articles address the cyber domain of warfare and the physical and virtual damage, military missions in cyberspace and threat characterizations. *CDR* readers will benefit from the scholarship of articles on the asymmetries of cyber conflict and distributed computing. The new research notes highlight defending democracy and multifactor authentication. I hope you will enjoy the new section and style of the research notes. This combination of research articles and notes will provide the variety needed to address the timely and interdisciplinary research in our field.

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



Colonel Andrew O. Hall is the Director of the Army Cyber Institute. He studied Computer Science at West Point, Applied Mathematics at the Naval Postgraduate School, and Operations Research at the Robert H. Smith School of Business at the University of Maryland. He has served on the Army Staff, Joint Staff, and deployed to the Multi-National Corps Headquarters in Baghdad, Iraq. He is a Cyber officer and was instrumental in creating the Army's newest branch.

And when you need another recommendation on what to read next, Dr. Kalberg and Cadet Ho's review of *Data and Goliath* details why Bruce Schneier's latest book should be on your bookshelf. This edition of the *CDR* will have its unveiling at CyCon U.S., our joint effort with the NATO Cooperative Cyber Defence Centre of Excellence. We look forward to continuing our interdisciplinary journey together in cyberspace. 🛡️

THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆

Cybersecurity: Focusing on Readiness and Resiliency for Mission Assurance

Rear Admiral Danelle Barrett

Mission assurance is the primary responsibility of all within the Department of Defense (DoD) and ultimately is Commander's business. It is imperative in today's rapidly changing information environment that Commanders understand how each of their primary missions is dependent on the operational platform for information for mission success. Having a comprehensive operational understanding of the cybersecurity readiness and capabilities of their information networks; including their ability to identify vulnerabilities and protect against threats, is as essential as understanding physical terrain in a kinetic operation. This involves a complete, end-to-end analysis of the information environment with an understanding of its technology, processes, and people. With that perspective, operational commanders can make informed choices on risk to their missions and implement means to continue operations in the face of an adversary determined to disrupt them.

Anyone who has worked in cyber defensive operations understands that it is a fool's errand to believe a network can be completely protected from adversary action. As the old saying goes "the most secure network is one that is turned off," but even that no longer applies to today's advanced digital and network technology and is an illogical option. Many approaches over the years have been tried to close vulnerability gaps and ensure survivability of networks to enable warfighting. Methods include improving network hardware, software and operating systems, communications equipment protocol and interfaces, and encryption of data and information transport systems. While all of these can result in limited success individually, they are best used in a holistic *Defense in Depth* combined approach that also incorporates the key elements of people and processes along with technology solutions. The most effective cyber defensive operations focus on maintaining the highest state of cyber readiness, being able to identify and protect against threats, ensuring redundancy, non-repudiation of data, confidence in the information, responding with speed and precision when attacked, and being able to 'fight through the hurt' using a combination of people, processes, and technology.

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



Rear Admiral Danelle Barrett has been in the Navy for 28 years specializing in communications, cyber, and information operations. She is currently assigned as the Navy Director for Cyber Security and the Deputy Chief Information Officer.

Understanding what needs to be defended for mission assurance, and to what degree, is the first step to building a more resilient warfighting platform. It starts with the operational commander and identification of their ‘no fail’ missions. These missions are not cyber or information missions, but the missions they are required to execute using all means available; ballistic missile defense, nuclear command and control, freedom of navigation, humanitarian assistance/disaster relief, amphibious assault, close air support, perimeter defense, logistics support, etc.

After the commander articulates their ‘no fail’ missions, they then identify ‘cyber key terrain’ supporting the operational platform for information used to successfully execute those missions. This analysis takes into account the cyber terrain required regardless of network classification as their missions often rely on multiple networks for success. Identification of cyber key terrain involves discussion of operational processes for those ‘no fail’ missions by their primary operators with technical cyber subject matter experts and cyber defenders. These conversations are essential to fully understand requirements such as information required and sources of those data and information. Analysis of cyber key terrain documents must encompass not only the information critical to mission success but how and where the information is generated, stored, transmitted, as well as how it is currently secured and protected. This is an end-to-end analysis of the operational, technical and system architectures with particular emphasis on identification of existing *Defense in Depth* measures. It will include analysis and identification of single points of failure that could be targeted by an adversary to disrupt command and control or impede the flow of critical information. It also includes documenting attributes of data/information on that cyber key

terrain such as timeliness of data, perishability, classification and releasability of information, redundant sources of information, and potential bandwidth limitations for missions extending to the tactical edge.

Once the cyber key terrain, including single points of failure, are mapped to the mission, the specific systems and their associated information exchange policies and procedures are identified. Careful examination of existing policies and procedures must be periodically executed to ensure there are no conflicts that could impede critical information exchange. Policies can be those of a technical nature such as orders for specific ports and protocol settings and access control lists on routers, rules set in cross domain solution devices, firewall configurations, and of a procedural nature such as how long systems and sensor logs are maintained and who reviews those, what is done with the data retrieved, how are systems administrators actions reliably and securely tracked and controlled to prevent insider threats.

In the Navy, a concerted effort has been in place since 2013 to counter adversary activity targeting the operational platform for information. Significant investments have been made in technology, processes, and personnel to detect, respond and recover from network attacks. This operational construct is termed ‘resiliency’ and goes hand-in-hand with cybersecurity readiness. As measures to assure resiliency of Navy networks continue to improve, operational commanders will have more tools at their disposal to maintain continuity of operations in cyber denied or degraded environments.

Processes for ensuring cybersecurity readiness and resiliency in networks should be automated to the maximum extent possible and data maintained in open standards formats to leverage emerging industry tools for improved network and configuration management and cyber defense. Artificial intelligence and state-of-the-art tools coupled with big data analytics could be tremendously powerful in proactively identifying potential malicious activity before an interruption or incident on a command’s cyber key terrain. Having a detailed understanding of the terrain and its system, and enabling technology agents to do the sensing and heavy lifting that systems administrators don’t have the capacity, intellectual ability, or time to do at the speed necessary to be proactive are key components of a *Defense in Depth* strategy for ensuring cyber readiness and resiliency.

This analysis of cyber key terrain mapped to the ‘no fail’ missions has benefits beyond mission execution. It is also can be used by those planning, programming and budgeting for future capabilities, and as noted to ensure proper cyber readiness sustainment of existing capability. Often it is difficult to articulate highly technical capabilities needed in the context of the end-to-end architecture and what the return on investment, operationally or fiscally, will be. Answering the question on every taxpayer dollar spent for cyber readiness and resiliency is important to guarantee we are using limited resources to the maximum benefit possible. Investments in automated solutions that are open standards

compliant, interoperable, easy to deploy and manage with minimal training or customization, and are scalable and useful in multiple operational environments will yield the most significant operational returns.

People are the critical third leg of the cyber key terrain analysis. Who are the cyber operators and defenders of that terrain? What is their state of readiness for executing cyber defensive operations and response actions? How are average users trained to ensure they understand that cyber defensive actions are an ‘all hands’ responsibility and that everyone is accountable to do their part to ensure availability and integrity of the operational platform for information supporting their ‘no fail’ mission?

In the past, network operators and telecommunications personnel were the primary forces used to execute these missions. As networks became more sophisticated, these forces were augmented by others who specialized in information assurance. In the last few years, the roles assigned to these forces have further expanded to cyber defensive operations that include proactive day-to-day operations to defend networks. Highly specialized forces within DoD that are trained to hunt adversaries on our networks and conduct incident response were added as well. In addition to the local Cyber Security Service Provider (CSSPs) that perform these functions on a daily basis on DoD networks, U.S. Cyber Command (USCYBERCOM) established the Cyber National Mission Forces (CNMF) in 2013 to execute cyber offensive and defensive operations. These forces, consisting of over 5,000 military and civilian personnel from all services, have specific teams assigned to perform cyber defensive missions. There are 68 Cyber Protection Teams (CPTs) exclusively trained and operating in this mission area protecting and defending DoD networks and conducting any other cyber defensive missions assigned by the Secretary of Defense.

Along with the day-to-day CSSP forces and the highly specialized CPTs, the average user plays an important role in the protection of cyber key terrain and their training cannot be overestimated. Cyber adversaries will use the easiest means to gain a foothold and attempt to penetrate DoD networks, and often rely on simple tactics, techniques, and procedures (TTPs), such as spear phishing, to gain initial access. While technical measures can be put in place to minimize the possible effectiveness of such TTPs, having a sophisticated workforce that is aware of what ‘normal’ on the network looks like and is suspicious of anything that deviates from that norm is important. Frequent and impactful training of network users is an important element of an overall *Defense in Depth* strategy. Additionally, holding users accountable for actions that violate established network policies is critical to instill a sense of ownership and individual responsibility for mission assurance. Leadership behavior in visibly following the rules is equally vital in setting the proper tone for cyber defense and ensuring it is seen as essential as other ‘all hands’ responsibilities like damage control on a ship or positive weapons control on the ground.

Once cyber key terrain is identified along with the technology, processes, and people needed to protect that terrain, operational commanders must then build in processes and procedures for mission assurance should that terrain cede to an adversary. How will forces operate if they are without their cyber key terrain, not just for a few hours but possibly for days or weeks? The cardinal sin of an operational planner is to assume away an enemy capability, and in the case of networks and cyber readiness today, we often see commanders make unsupported assumptions about what capability they will have and how they can fight through an attack. With advancements in automation to help with cyber situational awareness and response actions, commanders will have a more accurate, real-time cyber common operational picture and improved means to detect, respond and recover from attacks ensuring greater resiliency.

Operational planners along with cyber subject matter experts need to plan for operations in both a degraded or denied environment. For a degraded environment, this involves looking at several degrees of degradation and potential operational responses, either technical or procedural. In a denied environment, there are significantly greater challenges since the interconnectedness of our operational platform for information for 'no fail missions', and all the supporting operations are pervasively tied to our DoD networks. This includes weapons systems, industrial control systems and business systems like those specializing in logistics essential to enable warfighting operations. The ability for resiliency in all of those systems continues to progress as technology and processes evolve, but planners and commanders should understand their current capabilities and limitations and plan operations accordingly. The analysis should culminate in a series of comprehensive wargames that include second and third order effects which may become evident over time after periods of disruption or denial of cyber key terrain.

For example, after the 9/11 terrorist attacks, train service was interrupted across the nation as bridges and overpasses were inspected for potential terrorist activity. A second order effect of that shutdown was the inability to move chlorine, a chemical used to purify drinking water. The impact on drinking water was an unintended but potentially dangerous consequence of a required response action. The same type of analysis needs to be done for all military operations, particularly those that support combat operations for our 'no fail' missions. Risks can then be mitigated or at least understood by commanders who can then make informed choices about necessary actions for mission assurance.

Many services and organizations in the DoD are doing this analysis and building cyber readiness into existing capability to enable forces to 'fight through the hurt.' However, a clear understanding of commander's intent and priority for execution is imperative to synchronize effort, which can include potentially painful back to basics solutions in the event cyber key terrain is denied. A basic example of this is the reinstatement of celestial navigation instruction at the U.S. Naval Academy, which was phased out in 2006.

It had been deemed unnecessary due to shipboard technical solutions that could perform the navigation functions once required of humans. By once again providing this training, naval officers can continue to navigate by the stars using methods sailors have used for thousands of years should networked systems be compromised or fail.

When Commanders have decided upon means to ‘fight through the hurt,’ they need to codify those processes in doctrine and train to them during exercises. Commanders must clearly communicate where they can and will accept risk with those processes, and where they will not.

Technology can help as tools, sensors, and other capabilities will continue to improve, and operators need the ability to obtain and employ those capabilities on DoD networks quickly. As Admiral Mike Rogers, Commander, USCYBERCOM states, “Speed, precision, and agility” are paramount when it comes to operating and defending DoD networks. While acquisition reform is needed to allow for more rapid procurement and infusion of new and emerging cyber capabilities to outpace adversaries, DoD will work within the existing construct to field capability as quickly as possible. Identification of DoD’s “no fail” missions, along with the cyber key terrain that enables mission assurance, will allow the DoD to invest wisely now in the most impactful capabilities.

As technology in the digital warfare landscape continues to advance and adversaries, both nation state and non-nation state, become more capable of degrading or denying our access to and confidence in our operational platform for information, we must be innovative in our application of technology, processes, and people for mission success. The Internet and future Internet of Things (IoT), advancements in artificial intelligence, data analytics, and data use, and increasing integration of networked capabilities to include weapons systems and unmanned/autonomous vehicles, all pose opportunities for use against adversaries and challenges when used against us. The cost of entry in the information domain is cheap when compared with building traditional conventional forces. For example, billion dollar weapons systems significantly exceed the cost to an adversary of training a highly capable hacker who could achieve similarly destructive effects to our warfighting and operations.

Bottom line: Commanders must understand their cyber key terrain and its limitations and see it as an integral platform for their operations just like a plane, ship or tank. They can then, plan to use all the technology, processes and people at their disposal to maintain the highest state of cyber readiness and resiliency for operational success.🛡️

THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆

The Secret War Against the United States

The Top Threat to National Security and the American Dream

Cyber and Asymmetrical Hybrid Warfare

An Urgent Call to Action

T. Casey Fleming

Eric L. Qualkenbush

Anthony M. Chapa

ABSTRACT

Imagine if Pearl Harbor had been attacked and there had been no response from Washington.

This is the actual case today due to a highly sophisticated, mature, and stealth strategy perpetrated against the United States (US) by advanced military methods leveled at every sector and organization in our society. This includes private sector businesses, all government agencies, the military, and academia—every US organization operating with innovation, intellectual property, or sensitive data. The world is in significant conflict requiring the US government, military, and private sector to deliberately confront this national crisis or become permanently irrelevant. It is no longer “business as usual.”

Over the past three decades, as the US military trained in conventional, nuclear, and counterinsurgency warfare, the Chinese Communist Party (CCP) engaged and perfected over forty methods of warfare intended to permanently destabilize and weaken the US both economically and militarily. At the same time, China rapidly grew its economy and military without the required time or investment in innovation. The result is that the US is hemorrhaging its economic strength and relevance at the rate of \$5 trillion in lost total value each year, or one-third of the U.S. Gross Domestic Product (GDP). General (Ret.) Keith Alexander, former Director of the National



T. Casey Fleming serves as Chairman and Chief Executive Officer of BLACKOPS Partners Corporation, the leading intelligence, think tank, cybersecurity and asymmetrical hybrid warfare advisors to senior leadership of the world's largest organizations. He regularly advises the private sector, governments, agencies, military, Congress, and academia. Mr. Fleming is widely recognized as a top thought-leader, expert, and speaker in the areas of intelligence, national security, cybersecurity, and asymmetrical hybrid warfare. The Cybersecurity Excellence Awards recently named him *Cybersecurity Professional of the Year*. Mr. Fleming previously led organizations for IBM Corporation, Deloitte Consulting, and Good Technology. He served as the founding managing director of IBM's successful Cyber division, known today as IBM Security. Mr. Fleming earned his Bachelor of Science degree from Texas A&M University and participated in executive programs at Harvard Business School and The Wharton School.

Security Agency (NSA) and Commander of U.S. Cyber Command, referred to China's theft of American innovation and intellectual property as "the greatest transfer of wealth in history." Over time, a weakened US economy directly reduces the strength and effectiveness of the US military. Further, when a country is manipulated by an adversary to lose one-third of the value of its economy each year, it is at war.

ASYMMETRICAL HYBRID WARFARE

Clear and Present Existential Threat

Over the past thirty years, the US government and private sector have advanced their policy of full-cooperation, including substantial financial and technological investment in China, under the belief that they were moving towards a more democratic, free-market society while China played intentional misdirection and deception. In 1986, month number three, the Communist Party of China (CCP) officially declared Asymmetrical Hybrid Warfare (AHW) against the US and its western allies in its nation-state *Program 863*. This strategy commits all of China with its strict Communist military rule to engage in any and all methods to become on par with, surpass, and dominate the West at any and all cost. China's ultimate objective is to harvest and perpetuate the *Chinese Dream* through the extraction and extinguishing of the *American Dream*, the American way of life and ending Western dominance. The Chinese strategy is that after 200 years of Western global dominance, it is their destiny to reverse roles with the US and to relegate it to a forced supplier with a much lower quality of life. To underscore this strategy, China refers to the last century as "the century of great humiliation." It must also be emphasized that AHW strategy is rooted in Unrestricted Warfare or "war without rules."



Eric L. Qualkenbush is a member of the Board of Directors of BLACKOPS Partners Corporation. Mr. Qualkenbush is a former intelligence community senior executive with extensive experience leading large multicultural organizations through transformational change. He is an innovator who has created organization and programs that deal with the worldwide proliferation of weapons of mass destruction, insider threat, espionage mitigation, and competitive intelligence. During his CIA career, he led the CIA's principal training organization and the office that created and managed cover arrangements for all CIA personnel and others in the US government. Mr. Qualkenbush also managed undercover CIA operations in five overseas offices in the Middle East, and in Western and Eastern Europe. He also led pioneering work on mitigating insider threats in both private and public organizations.

DEATH BY A THOUSAND CUTS

The Modern Battlefield is Everywhere

AHW has been established as the future of modern warfare and business strategy across the globe. It is ultimate warfare that has many forms: economic warfare, transaction warfare, industrial warfare, drug warfare, and propaganda warfare, to name only a few. Each method is characterized by the non-utilization of military or conventional warfare that is typical of aircraft, ships, troops, and weapons. While China continues to aggressively develop and expand its military, it does so with the belief that if it must resort to the use of conventional or nuclear warfare, it has ultimately failed at achieving the enemy's capitulation through the combined methods of AHW. In the business sector, AHW has become the "*New Global Competitive Model*" where the "winner takes all." Soon, China will dictate transactions and pricing based on its market dominance. As businesses rush to move to "digital transformation" and "Big Data," each must perform a 180° cybersecurity transformation based on sensitive data protection and adversarial motives as a means to survive. Currently, AHW is the primary focus of our adversaries: China is, by far, the most successful at methodically executing all AHW methods, while Russia, North Korea, Iran, and India engage in relatively few methods at present. The strategy is to continuously inflict damage or cuts to every facet of American society just below the pain threshold where we choose not to act. We believe that China has achieved an estimated 750 cuts towards "death by a thousand cuts." (*Sun Tzu*)

Definition

AHW is characterized as unconventional, non-military, multi-method strategic warfare that is based



Anthony M. Chapa is a member of the Board of Directors of BLACKOPS Partners Corporation. Mr. Chapa is the CEO of Chapa Concepts, which provides threat and technology assessment for leading advanced technology and public sector organizations. Chapa Concepts also provides strategy and operational support to biometric access, security technology, and communications firms. Mr. Chapa retired from the United States Secret Service (USSS), Department of Homeland Security after a highly successful career, including Assistant Director and Chief Technology Officer responsible for the Technical Security Division. Mr. Chapa also served as Special Agent in Charge of the Los Angeles field office including leadership over the nation's premier USSS Electronic Crimes Task Force (ECTF). Mr. Chapa earned his Bachelor of Arts and Master of Arts in Political Science from St. Mary's University.

on deception and void of any rules between countries where economic and military power, strategy and tactics differ significantly. The attacking country exploits inherent weaknesses through numerous uneven and seemingly unrelated AHW methods that are designed to destabilize the unwitting target country for ultimate and complete economic and military submission. Extensive use of misinformation and plausible deniability are used to deceive and deflect suspicion of the strategy or its methodical advancement. Hybrid warfare is a military strategy that blends conventional warfare, asymmetric warfare, irregular warfare, offset warfare, non-linear warfare, and cyber warfare. AHW is rooted in unrestricted warfare (war without rules where “everything is fair play”) which is also described as “anything warfare.” *Source: BLACKOPS Partners Corporation—See Figure 1.*

Culture Disparity as a Strategic Weapon

It is important to note the striking contrast between the two cultures of the US and Communist China. It is this great divide that has contributed to China's manipulation and acceleration of AHW against the US. The CCP believes its “legalism” philosophy of supreme law and people are superior to America's constitutional democracy underpinned by justice, religion, a Creator, and “all men are created equal.” Since 1949, the CCP have controlled all aspects of China's commerce, military, and daily life where intellectual property is state-owned, all data is controlled, and it is the national duty of all citizens to support the regime, including all aspects of espionage. The Communist culture is further defined not by “winning vs. losing”; rather, “*living vs. dying.*” It is this extreme belief that underscores China's support for AHW in its conflict with the US. Another distinction is that the CCP controls every business transaction with US companies. In many

cases, the CCP resembles a powerful organized crime faction, through its shell business partnerships and facades. There is no distinction between China's organized crime, military, or government. This places every US business partnership or transaction with China at extreme risk.

Critical Role of Intelligence

China's uncompromising commitment to AHW demonstrates a national objective to destroy the US and its Western allies. The critical nucleus that drives the AHW strategy is the complete dependence on stolen innovation, intellectual property (IP), sensitive data, and military secrets—namely intelligence. For over thirty years, China has orchestrated the most impressive and sophisticated strategy with an intricate global network of espionage and industrial theft to fuel AHW. In recent years, an emboldened China has demanded the complete surrender of all intellectual property during the process of contracting current international business transactions. Conversely, intelligence plays a critical role for the US to gauge the executional success of AHW, changes in strategy, and individual and cumulative damages.

Cyber Warfare as the Key Accelerator

China has successfully intertwined Cyber warfare as the key AHW accelerator due to its relatively minimal investment and the difficulty of attributing actions to a specific actor. At the same time, cybersecurity remains fundamentally broken in the US and the West due to failed cyber strategies, lack of awareness of AHW, lack of accountability, overconfidence, and overdependence on inherently fallible cybersecurity products. This is made clear by the “new normal” of the increased trend in number, frequency, and resulting total damages from cyberattacks.

Current estimates place global cyber losses at \$6 trillion by 2021, with expectations that this will increase further in the future, according to Cybersecurity Ventures. Cyber warfare and cybersecurity have become a “whole of society” challenge that requires a unified, elevated strategy and 180° approach to combat the morphing threat. As we examine today's cybersecurity environment, we are looking through the wrong end of the telescope. It is only in the context of AHW that we can begin to fully understand cybersecurity's critical role for successful defense, protection, and resolution. We have learned to treat cybersecurity first and foremost as a human problem and a senior leadership challenge, not solely an IT issue.

Call to Action

The US must immediately increase awareness, positive action, and accountability in all sectors and at all levels through creating a unified and aggressive approach in responding to the advancement and threat of AHW. The following recommendations are put forth:

- ▶ Immediately establish the Asymmetrical Hybrid Warfare Center (AHWC)

- ◆ Public-Private Partnership Center (P3C) coalition, U.S. university-based with Department of Defense (DoD) participation
- ◆ Independent leadership and reporting structure as a resource-focused, support entity charged with maximum efficiency (reporting to the U.S. Executive Branch or U.S. Senate Select Committee on Intelligence)
- ◆ Constituents: USG, Pentagon, Congress, private sector, academia, and US Allies
- ◆ Mission: strategy, intelligence, counterintelligence, research, tracking, analysis, awareness, training, AHW-countering recommendations to constituents (e.g., foreign acquisition of assets determined to be harmful to US economy or military, false shell companies, espionage reporting database, misinformation generation, spyware)
- ◆ Cybersecurity consortium clearinghouse with anonymity scrub: intelligence at a level higher than today with a focus on advanced attack methods for early warning and resolution
- ◆ DarkNet research and triangulation, active surveillance as adversaries increasingly exploit this platform
- ◆ Regular release of evolving cybersecurity attack methods and best practices
- ◆ No organization or entity today is positioned for this center or mission
- ▶ Transformational culture change to protect innovation, IP, and cybersecurity sensitive data
- ▶ AHW executive briefing and exercise for key US and Allied organizations (government, military, private sector, and academia) to train in AHW strategy, methods, and countering techniques

Summary

The persistent engagement of Asymmetrical Hybrid Warfare (AHW) will continue to grow as the preeminent threat to US national security and will characterize the future focus of each of our adversaries. Asymmetrical/Conventional/Nuclear is the new continuum of modern warfare. The Russian hacking of the 2016 U.S. Presidential election clearly demonstrates the shift of AHW to the forefront and the relative effectiveness of a single act and method. All sectors of US society: private sector economy, the government—especially Congress, military, and academia must increase its awareness of highly advanced AHW, provide accountability, and routinely engage in effective countermeasures to secure and protect the future of the United States.🛡️



Figure 1. The 'New' Global Competitive Model

The views and opinions expressed in this paper are those of the author(s) alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DoD) or any agency of the U.S. Government.

Digital Network Resilience: Surprising Lessons from the Maginot Line

Ray A. Rothrock

ABSTRACT

For most of us today, the phrase “Maginot Line” is a stale but cruel joke, if not just some vague memory from a high school history class. It is well-worn metaphoric shorthand for any defensive measure firmly believed to provide excellent protection, but that is in fact quite useless. Actually, worse than useless—because building a Maginot Line creates the complacency of a false sense of security.

There was a time, of course, between the two world wars, when the Maginot Line was more than a phrase. It was a reality of excavated earth, reinforced concrete, and powerful artillery: “an immense project comprising 100km of tunnels, 12 million cubic metres of earthworks, 1.5 million cubic metres of concrete, 150,000 tons of steel and 450km of roads and railways.”^[1] The brainchild of French Minister of War André Maginot, it was built between 1928 and 1938 along much of France’s eastern border and cost 3 billion francs^[2] in the 1930s, which is about 3.7 billion 2017 U.S. dollars. The finished fortification complex had 589 principal structures above ground plus some 5,000 small detached blockhouses. Connecting many of the principal buildings were subterranean tunnels, barracks, and storage facilities. It was an ambitious marvel of military engineering.

What did the people of France get for their \$3.7 billion investment?

On the face of it, very little. The conquest of France in 1940 took just forty-six days. When the nation surrendered, it had lost not only the so-called Battle of France, but World War II itself. The German invaders suffered about 163,676 casualties, killed and wounded, but French military casualties totaled 2,260,000, killed, wounded, or made prisoner.^[3]



Ray A. Rothrock is CEO and chairman of Red-Seal Inc., a company providing enterprises with a network modeling and risk scoring platform that measures and improves resilience to cyber events and network interruptions. He is partner emeritus of Venrock; and a member of numerous boards including CheckPoint Software, U.S. Department of Energy GAIN, Roku, Inc., Tri Alpha Energy, Inc., Team8, and UTIMCO, a \$40B public endowment for the University of Texas and Texas A&M University. He also is a member of the Corporation of the Massachusetts Institute of Technology.

In 2017, Ray led conversations at the Milken Institute Global Conference, the SXSW Conference, and the NACD Global Board Leader's Summit. He also participated in the 2015 White House Cybersecurity Summit. Ray holds a BS in Nuclear Engineering from Texas A&M University, a MS in Nuclear Engineering from the Massachusetts Institute of Technology, and an MBA with Distinction from Harvard Business School.

On the face of it, the Maginot Line represents a spectacularly poor return on investment (ROI) and richly deserves to survive in language as mocking shorthand for a disastrous monument to a collective national posture of heads-in-the-sand.

What served for many years after World War II as a durable label for any instance of delusional defensive strategy has become in the digital age an Internet meme signifying head-in-the-sand cybersecurity. A recent Google search on the phrase “Maginot Line cybersecurity” produced dozens of articles with titles like “Cybersecurity’s Maginot Line,”^[4] “Don’t Build a Maginot-Line Cybersecurity Defense,”^[5] “No More Cyber Maginot Lines: We Need to Hunt Down Hackers Before They Strike,”^[6] and “Avoiding Maginot Line Mentality: What False Assumptions Underpin Current Cyber Security Strategies?”^[7]

You will find some thoughtful and valuable ideas in this “Maginot Line” genre of cybersecurity writing. Go ahead and skim. But I must caution you: all of the articles and reports in this Maginot Line group suffer from the same flaw. All base a complex argument on the same unexamined meme. The historical, strategic, and doctrinal realities behind the Maginot Line meme reveal what serious military historians have long understood, but nobody else has bothered to investigate. The Maginot Line has been getting a bad rap.

Now, before I set down another word, let me assure you that this article is not really about the Maginot Line. It is about the single most critical mistake most businesses make when they set their cybersecurity spending priorities: prioritizing security over resilience.^[8] Before I define both security and resilience, it really will help if we understand the reality behind the Maginot Line meme. Allow me, then, just a few more sentences on this episode of military history.

The Maginot Line's champion and namesake disclaimed any intention of building in France the equivalent of the Great Wall of China "Instead," André Maginot wrote, "we have foreseen powerful but flexible means of organizing defense, based on the dual principle of taking full advantage of the terrain and establishing a continuous line of fire everywhere."^[9] Maginot had served as a sergeant during World War I and was awarded the *Médaille militaire*, France's highest military honor.^[10] This minister of war was neither a bureaucrat nor a theorist. He was a combat veteran with real-world experience, who understood that no passive wall would keep out a determined enemy. And so, the Maginot Line was not a wall, but a coordinated set of active defenses designed not to stop an army, but to slow it down by killing as much of it as possible. Its purpose—its true purpose—was to create strategic and tactical opportunities for organizing not just a defense, but effective counterattacks. Military historian Julian Jackson, wrote, "the Maginot Line had never been conceived as a ... Great Wall of China sealing France off from the outside world. Its purpose was to free manpower for offensive operations elsewhere."^[11]

It pays to parse Professor Jackson's final sentence. The "purpose"—the top priority—of the Maginot Line was not defense but offense to "free manpower for offensive operations." The Line's defensive function—its security function—was secondary to its offensive function, which we can call resilience. The French plan never assumed that the Maginot Line was an impenetrable firewall. It was, rather, what military theorists, as well as warfighters, call a force multiplier. Force multipliers "work to optimize force capabilities ... The concept of force multipliers is a key element of U.S. military doctrine that asserts we can fight with limited resources and win."^[12] Used correctly—not as a security device (a "wall"), but as a force multiplier (a device to enhance resilience), the Maginot Line should have been instrumental in defeating the Nazi invasion of France:

The true flaw in French military strategy during the opening days of World War II lay not in reliance on the Maginot fortifications but in the [French] army's neglect to exploit the military opportunities the Line created. In other words, the border defense performed as envisioned, but the other military arms supported it insufficiently to halt the Germans. The French Army squandered the opportunity not because the Maginot Line existed but because they failed to utilize their own defensive plan properly.^[13]

Instead of following the plan, which was to prioritize resilience to enable an effective offensive operation against the invaders, the French commanders chose instead to hunker down behind the Line, as if it were an inert and impenetrable wall. *The French leadership prioritized security over resilience.*

For anyone charged with protecting digital networks and the data that flows across them, the strategic error of the French commanders in 1940 is the real lesson behind the shallow and misleading Maginot Line meme: *Understand cybersecurity as more than*

security. Effective cybersecurity plans for, provides for, and executes on both security and resilience—with the greater priority always given to resilience: the ability to fight back, quickly and effectively.

André Maginot and the other original planners of strategic doctrine around the line of fortifications that was posthumously named for him understood that fortifications by themselves will not stop an invasion, but they can facilitate defense through a counteroffensive. These men would have understood former James B. Comey (at the time FBI director) when he told CBS *60 Minutes* in October 2014, “There are two kinds of big companies in the United States ... those who’ve been hacked ... and those who don’t know they’ve been hacked.”^[14] They would have understood that no “wall” is sufficient to prevent penetration of a nation or a digital network. They would have understood that, while security is a necessary, even essential, tactic, it is not a sufficient strategy. It must be applied in coordination with resilience.

We don’t know if Maginot and his colleagues were familiar with Sun Tsu’s ancient maxim that “a victorious army wins its victories before seeking battle; an army destined to defeat fights in the hope of winning.”^[15] We suspect Director Comey was familiar with it. In any case, the maxim applies to both France in 1940 and digital networks today. The Maginot Line was planned as part of a war-winning strategy on the assumption that nothing could absolutely prevent an invasion. The failure of the Line was due not to a faulty plan, but to the substitution of the mere “hope of winning” for the faithful execution of what was a reasonable plan. Concerning cybersecurity, Comey’s statement implies that no defensive measure—no mere security approach—can absolutely prevent a breach. The proof of this is that the battle against hacking has already been lost. If you don’t know that your organization has been hacked, it has been hacked without your knowing it. Since security is therefore insufficient (though necessary), you need a means of digital warfighting that is effective against the attacker you know as well as the attacker you do not know. You need a means of effectively responding to the penetration that has already occurred, the breach that is currently in progress, and the breach that will inevitably happen.

The most profound implication of Comey’s remark is that those of us responsible for protecting networks need to understand the basic difference between security and resilience. Security is analogous to the “wall” function of the Maginot Line. It is about preventing an attack. This is a necessary function and a laudable objective, but it is insufficient for the same reason that former Secretary of Homeland Security Janet Napolitano gave (when she was governor of Arizona in 2007) for not building a border wall to stop illegal immigration: “As I often say, ‘You show me a 50-foot wall, and I’ll show you a 51-foot ladder.’”^[16] It is not sufficient to hope that a wall, security alone, will bring victory. Resilience, the other component of effective cybersecurity strategy, neither offers nor depends upon hope. Resilience is, in fact, creatively pessimistic in assuming that a large number of cyberat-

tacks will inevitably be directed against any and every organization, that security devices will inevitably fail to stop a significant fraction of those attacks, and that management's top cybersecurity priority should be reducing the volume and severity of damage and loss as well as staying in business or on mission during a breach. It is in such a reduction of impact that we find the likelihood not only of survival and recovery but of even continuing to operate without interruption. Resilience is about standing up to do business while fighting back and recovering.

A cybersecurity strategy that prioritizes resilience includes, at minimum, six elements:

- 1. It intelligently assesses data assets for protection.** Resilience must be framed not as an IT department security strategy but as a whole-enterprise business strategy. Security imperatives do not necessarily coincide with the imperatives of resilience. For example, arbitrarily limiting customer access to data may increase security, but it also impedes the ability to do business. A hobbled organization is a less resilient organization in that it is a step closer to failure. Resilient organizations strategically prioritize access by assessing data assets in terms of network accessibility, critical sensitivity of information, value of proprietary intellectual property, and customer need-to-access.
- 2. It focuses on performance outcomes rather than infrastructure protection.** Resilient organizations devote the greatest resources to protecting what keeps them operating—that is, performance for “customers” (defined as everyone the organization serves) and achieving the assigned mission. Infrastructure exists to enable performance, not vice versa. Resilient strategy always balances performance against security.
- 3. It prioritizes detecting breaches and responding to them.** Resilience assumes the reality that bad things are happening. Security seeks to prevent bad things from happening. The first engages a reality. The second takes certain defensive steps in the hope of evading or postponing that reality.
- 4. It creates understanding of how data flows into, out of, and through the organization's networks.** Without this understanding, it is impossible to apply appropriate and effective controls on data access. In contrast to resilience, the imperative of security is to control (in other words, to restrict) the flow of data.
- 5. Resilience engages the entire organization.** Security strategies tend to focus on IT technology. Resilience engages the people who use technology. Its objective is to create an organizational culture of resilience, which enhances both security and the capacity to stand up under attack, continue operating during a breach, and rapidly recover in the aftermath.

6. Most of all, resilient strategy declines to waste resources on defending perimeters in the “hope of victory.”

In 1940, France had a perimeter to defend. Today’s extensively connected, intensively interactive digital networks ultimately have no perimeters. Today, attacks come from everywhere, from without and within. The multiplicity and complexity of connections present both unprecedented opportunities and unprecedented risks. Every organization understands that the quality of its product is only as good as the quality of its supply chain. If you’re in the business of making lemon meringue pies, your pies can never be better than what your lemon suppliers sell you. By the same token, an organization’s network is only as secure as the networks with which it connects.

World War II may have been the last war with definable fronts—distinct perimeters. Perhaps, then, the stewards of today’s digital networks are better served not by the 1940s metaphor of the Maginot Line, but by the more recent reality of insurgent warfare. During the 1960s and 1970s, the Vietnam War forced the U.S. military to transform itself into an organization capable of fighting armed conflicts in battlespaces without fronts. This is the situation for today’s digital network users and managers. The complexity and multiplicity of today’s Internet, which includes the vast network of the Internet of Things (IoT), forces organizations to discard the notion of any network “perimeter” to defend. As University of Cambridge computer scientist Robert Watson has put it, “The default assumption is that everything is vulnerable.”^[17] The only realistic response to this new reality is for digitally transformed organizations to create the necessary resilience to sustain high performance while identifying and neutralizing intruders both coming and arrived. 🛡️

NOTES

1. William Allcorn, *The Maginot Line, 1928-45* (London and New York: Oxford University Press, 2003), 9.
2. Robert Kuttner, "The Economic Maginot Line," *The American Prospect* (August 11, 2011), <http://prospect.org/article/economic-maginot-line>.
3. Micheal Clodfelter, *Warfare and Armed Conflicts: A Statistical Reference to Casualty and Other Figures, 1500-2000* (Jefferson, NC: McFarland and Company, 2002), 489.
4. Fire Eye, "Cybersecurity's Maginot Line: A Real-world Assessment of the Defense-in-Depth Model," <https://www2.fireeye.com/real-world-assessment.html>.
5. Eric Holdeman, "Don't Build a Maginot-Line Cybersecurity Defense," *Emergency Management* (March 14, 2016), <http://www.govtech.com/em/emergency-blogs/disaster-zone/dont-build-a-maginot-line-cybersecurity-defense.html?flip-board=yes>.
6. Nate Fick, "No More Cyber Maginot Lines: We Need to Hunt Down Hackers Before They Strike," *Defense One* (June 5, 2016), <http://www.defenseone.com/ideas/2016/06/no-more-cyber-maginot-lines-we-need-hunt-down-hackers-they-strike/128823/>.
7. Editorial Team, "Avoiding Maginot Line Mentality: What False Assumptions Underpin Current Cyber Security Strategies?" *CrowdStrike Blog* (April 14, 2015), <https://www.crowdstrike.com/blog/avoiding-maginot-line-mentality-what-false-assumptions-underpin-current-cyber-security-strategies/>.
8. In a survey of 200 corporate CEOs conducted by RedSeal, Inc., in September 2016, 50 percent reported prioritizing "keeping hackers out of the network" while "just 24 percent were concerned with building capabilities to deal with hackers who have successfully breached their network's perimeter defenses." (RedSeal, "Cybersecurity Perception Survey," conducted by Finn Partners, September 2016; "RedSeal CEO Survey: Summary & Key Findings," <https://www.redseal.net/wp-content/uploads/2016/12/RedSeal-CEO-Survey-Executive-Summary.pdf>, 1.
9. Charles River Editors, *The Maginot Line: The History of the Fortifications That Failed to Protect France from Nazi Germany During World War II* (N.p.: Charles River Editors, n.d.), Introduction; Kindle ed.
10. Laura Lee, *The Name's Familiar II* (Gretna, LA: Pelican Publishing Company), 226.
11. Julian Jackson, *The Fall of France: The Nazi Invasion of 1940* (New York: Oxford University Press, 2003), 27.
12. Major David S. Powell, Field Artillery, *Understanding Force Multipliers* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 1990), <http://www.dtic.mil/dtic/tr/fulltext/u2/a234153.pdf>, 1.
13. Charles River Editors, Introduction; Kindle ed.
14. James B. Comey, quoted in Scott Pelley, "FBI Director on Threat of ISIS, Cybercrime," *60 Minutes* (October 5, 2014), <http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/>.
15. Samuel B. Griffith, trans. and ed., Sun Tzu, *The Art of War* (London and New York: Oxford University Press, 1963), 87.
16. Glenn Hurowitz, "Who Me a 50-Foot Wall, and I'll Show You a 51-Foot Ladder," *Grist* (November 21, 2008), <http://grist.org/article/napolitano-knows/>.
17. The Economist, "Why everything is hackable," *The Economist* (April 8, 2017), 69.

Combatting the Rise of ISIS 2.0 and Terrorism 3.0

Oz Sultan

ABSTRACT

In the early 1990s, a then-nascent al-Qaeda took steps to redefine both the nature of conflict and the nature of ideological foundations for waging war. The United States military deployment to the Middle East following the Iraqi invasion of Kuwait drove Osama bin Laden to deviate from both defined Islamic theology and fiqh (Islamic jurisprudence) and take a more 'guerilla' approach to combating what he saw as US aggression. Bin Laden deviated from both religion and traditional conventions of war to declare US Troops, supporting contractors, Arab troops, and even fellow Muslims and non-combatant villagers as enemies of al-Qaeda—should they prove to be obstacles to al-Qaeda's goals of regional control and hegemony.

This new characterization of non-combatants and Muslims within conflict zones as the 'enemy' opened up horrific new doors to civilian casualties and collateral damage while setting the stage for the transformation seen across terrorist groups in the past decade.

Counterinsurgent battles from hegemonic struggles waged by waning colonial powers across Africa and Asia in the 1950s and 1960s gave way to the education of militants and insurgent groups from the 1970s-1990s that resulted in well-trained geographically disparate insurgent and terror organizations. These organizations that would traditionally stay relegated to regional conflicts became connected through the Internet and social web starting in the mid-2000s.

Through the 1990s-00's, we witnessed the al-Qaeda (EMEA) threat and the growth of Al-Shabab (MEA), Abu Sayyaf (Philippines), Jemmah Islamiyah (SE Asia), Wilayat Khorasan (Afghanistan, now ISIS-K) and Boko Haram (Africa). The attitude of these groups—some based on Salafist ideals—moved away from religious ideology and



Oz Sultan is a Tech and Marketing Industry veteran with 20 years' experience developing innovative solutions for Brands and Fortune 100 companies. He is also at the forefront of American Muslim affairs, as well as diplomatic and interfaith engagement.

Over the past ten years, Oz has leveraged social media signaling and analysis of trend and social media data to focus on Big Data analysis and how patterns can aid in solving complex problems around us.

Oz has developed a Digital Anti-ISIS framework and counter-radicalization and disruption methodology for stopping online terror.

One fundamental aspect of his work is to get governments and corporations to see the risk of Cyber Terrorism, Crypto Ransom and Social Media converging in what he calls the "greatest risk facing America."

Recently he was a counterterrorism, social media and Big Data advisor to the Trump Campaign. He is a regular contributor to *IJR*, *TexasGOPVote*, *The Ish*, and *Newsmax*.

towards a type of cult-like indoctrination methodology. The ideology that could quickly radicalize and weaponize youth fighters and conscripts became essential elements in building insurgent movements.

Adding a degree of complication to this new environment was the nature of different sectarian groups developing within a single conflict arena. For example, during the Iraq War in 2004, there were between 63 and 68 active insurgent and separatist groups. Many had territorial or rights aims, while other groups aligned with different ethnic and Islamic religious sects. This move towards a diffused organization and more cause-oriented sectarian division allowed for the ground transformation that we couldn't have predicted.

Al-Qaeda began moving towards new radicalization methods in the mid-00s. While initially in Arabic, by 2015 al-Qaeda was publishing an English Language Magazine called *Inspire*. *Inspire* has moved from al-Qaeda recruitment, travel and training to syndication of *Anarchist's Cookbook*-style terror tools with *Turner Diaries*-style rhetoric in a magazine that has the publication quality of *Vogue* magazine. Al-Qaeda affiliates also publish regional publications for the Indian Subcontinent (AQIS), as well as other global regions.

The Social Media Transformation of Culture

Anyone born before 1980, which covers Great War, Boomer, Gen X and part of the Millennial Generations, had a transference of cultural, ethnic and religious traditions through oral literary tradition; church, synagogue or mosque; community; and family. But Millennials (born mid-80s-90s) Generation Z (born mid-90s-00s) and the Homeland Generation (born 2005-on) have an entirely different understanding of life, culture and religion because of the Internet and new methods of social

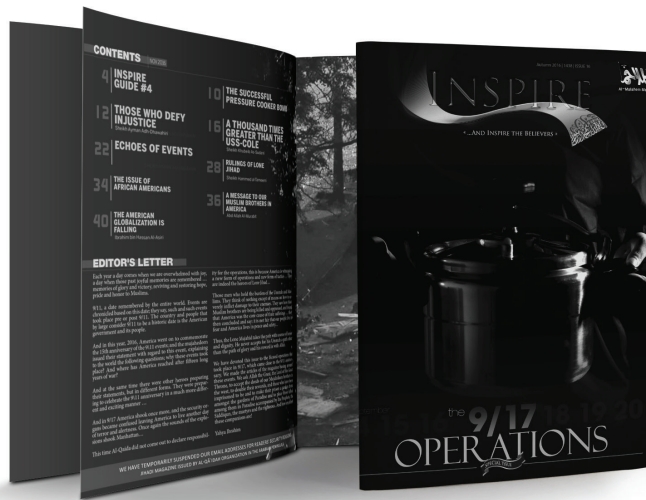


Figure 1. For illustrative purposes only, *Inspire Magazine* is an example of propaganda used by al-Qaeda to broaden its reach and further its cause.

engagement. Further, past generations had different cultural beliefs from location to location, but due to the Internet and the social web, people now have shared experiences across global regions.

Almost 30% of Millennials and a larger percentage of Generation Z were not raised with a religious upbringing and did not have the same cultural or vocational expectations that their parents had.

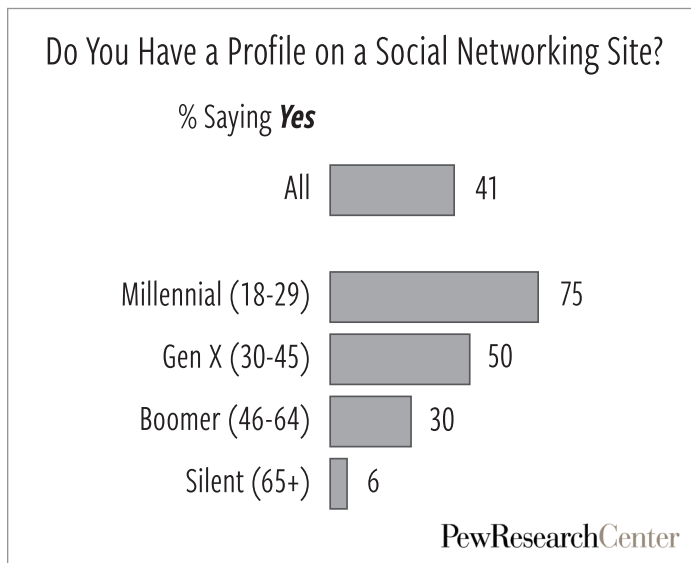


Figure 2. Social Networking

This has given rise to dramatic cultural and experience transference gaps between generations. It has also led to massive shifts in society. A brief survey from the Sultan Interactive Group of Occupy protesters in 2011, showed very little association or understanding of Freedom Riders or social movements of the 1960s, and more focus on disrupting established economic structures.

Today, seventeen to thirty-five year olds are more prone to receive influence, identity, and opinions from social media and social media influencers within their social networks. Social media itself has given way to new social norms, changed expectations and the establishment of online culture jamming. This trend is both local and global. At the same time because of this global technological transformation, information and trends now take minutes to spread online where they used to take days to spread just a decade ago. As people have formed digital groups and tribes, segments of society who once found themselves ostracized now connect with others in this digital playing field.

The Rise of the Jillennial

In the 2000s, al-Qaeda conscripts originated from marginalized Salafi and Deobandi communities in Europe, however, the nature of jihadist recruitment and rhetoric changed completely with the rise of ISIS. ISIS began to recruit from a broader base of individuals who largely had little or no relationship with Muslim communities and often no understanding of Islam.

Social Media dissonance or, detachment from society and a readiness to look for disruptive ideas, typifies the nature of millions of people online today. The increase in secularism globally has also complicated the landscape with many individuals in their 20s having few expectations or direction for themselves.

Last year, our Sultan Interactive Group conducted a one-year analysis of 80,000 ISIS-leaning or ISIS-sympathizing Twitter accounts. This included looking at the nature of Twitter account holders, demographics, age, sex, ethnic origin, education, income, lifestyle, religious affiliations, political engagements, previous criminal records, the percentage of youth in jails, the conviction for crimes as well as a societal disengagement index.

Key findings from the research:

All the recent attackers in France were in their twenties, both of the attackers of San Bernardino were in their twenties as well, so were the majority of attackers in Europe post-2001, from the 2004 Madrid attacks to the 7/7 subway bombings in London, as well as the actors behind numerous foiled attacks. Millennial Jihadists (Jillennials) become a good point to start our data exploration for understanding what they do differently that would help us pick their online patterns and behaviors.

Millennials are more connected to their parents than their parents were connected to their grandparents; parents pay 59% of millennials' cell phone bills, and they do not mind returning to their parent's house and asking for financial help. Twenty-eight percent of millennials get married between the ages of 18 to 32 versus 48% of the baby boomers generation. They are less religious (36% versus 61% of boomers), less patriotic (49% versus 81%), surprisingly less environmentalist (32% versus 44%) and more supportive of LGBT rights (51% versus 32%).

We have found millennials in Europe have 250 friends on average on Facebook, while individuals with a probability of radicalization have less than 100. We found 55% of European Facebook users share their selfies versus almost 1% for the second group of potential ISIS recruits. These millennials can spark a riot in less than two hours using Twitter only, and we call it #HashtagIncitements. If it is among the closely connected cohort of potentially radicalized youth, it can happen within 20 minutes or so.

Key findings of our research validated several conclusions:

- ◆ **First, the World of War, Social Media and Cyber have intersected. We need a new Crypto Social Cyber Approaches to SOPs, Defensive Postures, and Military Theatre responses:**
 - ◉ US Coalition-supported troops, Free Syrian Army (FSA), Kurd (YPG), Russian, and Iranian-backed forces in Syria are often quickly outed on social media with pictures and video disclosing operations. Cyberwarfare is often compromised by social media responses, and with the ease of access to Crypto Ransom weapons, we see operational risks arise.
 - ◉ Radicalization exists in a virtual landscape, with virtual conversations and synthetic inducements for people to radicalize. Most often there is the creation of virtual power structures in cyberspace that allow power relations that do not exist in the real world.
 - ◉ We can imagine an avatar who relies more on emoticons than words, taking a seat next Ayman al-Zawahiri or Abu Bakr al-Baghdadi. While the players behind the character may change, the digital persona remains the same, thus providing an immortal inspiration to admire and emulate.
- ◆ **Secondly, Religion has little or no bearing on the likelihood that a marginalized Millennial or Gen Z'er will be radicalized:**
 - ◉ The majority transition from secular to radical. The people in this group do not attend local mosques or even talk to community leaders or neighbors or even the people from their home country. They sit in the dark, learning, and practicing online until they are ready to act. The majority of the radicalized people are off-the-radar for years.

♦ **Thirdly, *The Process of Radicalization opens a Pandora's box:***

- ◉ Even someone who does not find the courage to go out and launch an attack helps by producing propaganda videos and distributing the planning material online. With dozens of Online Encouragements and a higher ordinance in the artificial chain of command, anyone can become a commander-in-chief of their sleeper cell that does not exist in reality.

As such, the profile of the Jilennial is different from profiles that have been previously developed. These are validated by arrests over the past 24 months.

Typically they are:

- ♦ Millennial (21–34), Disenfranchised
- ♦ Western (White) or Second Generation Immigrant
- ♦ Secular (Non-religious)
- ♦ Looking for Meaning (ISIS baits for this)

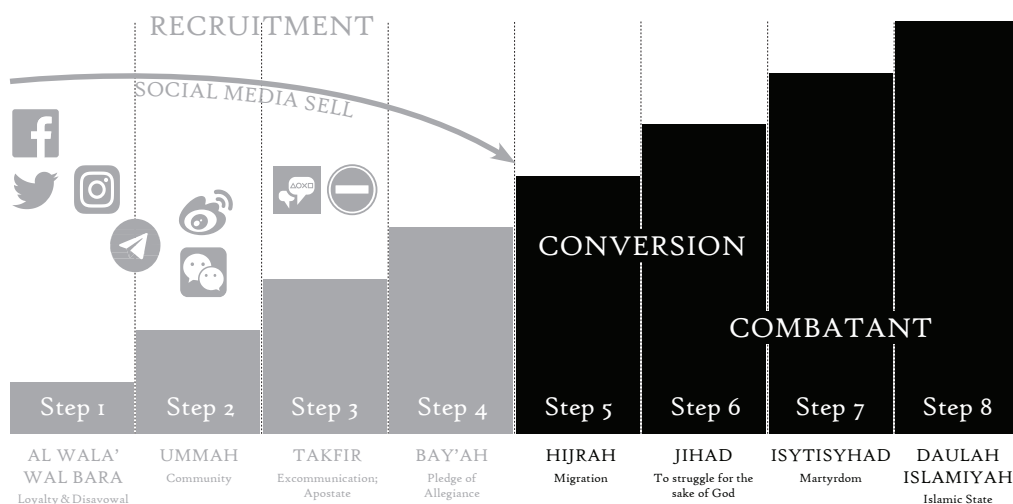


Figure 3. ISIS's Online Recruitment Process

Globally and within the US, we see an increased need to educate, engage, and defend against this risk profile. We live in a world of social media marketing campaigns where Instagram posts, video game mods, and Twitter are being used as tools to recruit. These campaigns are so successful they even ensnared a disenfranchised and marginalized US military member in July 2017.

ISIS's primary recruitment methodology leverages online social media tools and messaging that run like marketing campaigns similar to the best marketers in America. Quilliam International estimates that ISIS operates a network of about 1,000 social and digital media operatives globally, making their staff more numerous than many large public relations agencies.

Their recruitment process starts with glossy English-language publications like *Dabiq*, and social seeds and hashtags across the social web. Dedicated websites on the Darkweb and readily available ISIS propaganda online are coupled with a recruitment process that is socially geared towards the disenfranchised millennial audiences.

The Social Media phase of ISIS's recruitment process

Once a prospect starts communicating with an ISIS recruiter, they are quickly sold a 'bill of goods' that include incentives, opportunities to lead or to find a "meaningful life and place". The recruitment process involves an initial pledge to Islam, as well as the standard cult tactics of cutting off friends and family for a new "peer and social group". Once this occurs, they are led to excommunicate their family, all religious elements in their life, and take an oath of allegiance to ISIS.

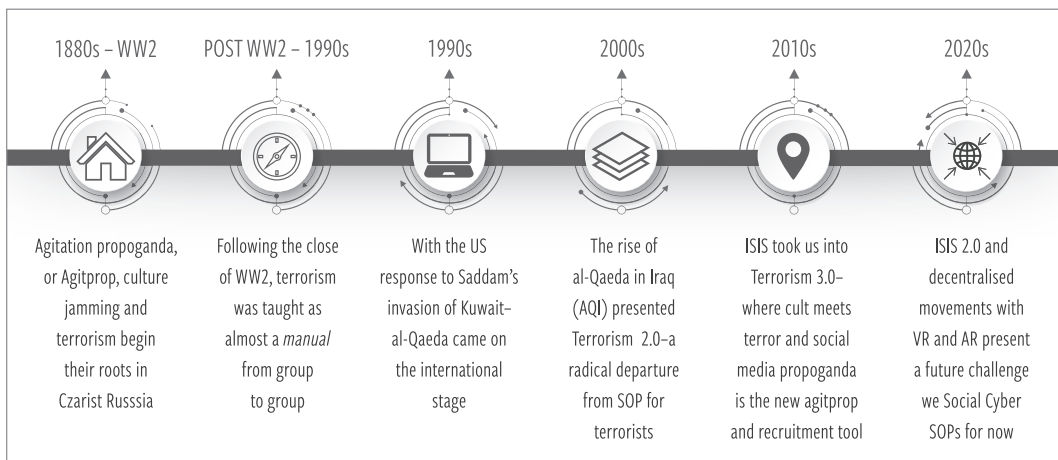


Figure 4. Terrorism 3.0 and ISIS 2.0

To disrupt this process, we must focus on new strategies of engagement, social media SOPs, and develop guidelines for remediating social media, marketing, and recruitment threats that live in the same real-time, online terror ecosystem. Beyond recruiting, people, nations, and corporations now face the same degree of risk. Manchester is a case study in the impacts of people, a country (UK), a town (Manchester), businesses, physical property (SMG, the arena operator) and a pop icon (Ariana Grande).

The Rise of ISIS moved us from the world of Terrorism 2.0 that used the Internet to Terrorism 3.0, which is fully immersed in social media. ISIS has developed World War Two style propaganda campaigns that now play out in News (AMAQ agency and global coverage), Video (YouTube, News and Terror updates), Audio (sound clips and audio tweets), Social (Facebook, Instagram, Snapchat, Twitter, Weibo, etc.), Video Game mods (ARMA 3) as well as in social campaigns tied to #hashtags. While the US may be winning the ground war, we need new strategies to combat ISIS online. If ISIS can have four glossy online media magazines in addition to sophisticated online posts, video, tweets and retweets from a single IED attack, then the West needs to bridge the social media gap through cyber-focused Intel to fight back effectively.

In the Spring of 2017, ISIS put out a call to their recruits for attacks focused on civilians in Europe, the US, and Australia. This call was fulfilled with attacks in Manchester, London, France, and a bomb attempt in Brussels during the summer of 2017.

As ISIS was able to spread unabated over the past six years—mainly due to global hand-wringing and bureaucratic indecision over Russian and Iranian involvement in Syria—ISIS expanded their footprint. Wilayat Khorasan became ISIS-K in Afghanistan, and the ISIS involvement with Abu Sayyaf and the Maute Group in the Philippines shows a new strategic partnership. ISIS is focused on a grassroots expansion—raising the challenge of an ISIS 2.0 once their Deir Ezzor and Raqqa strongholds are eliminated. ISIS is partnering with regional terrorist groups to extend their reach, creating a global fallback network when the Caliphate collapses in Syria.

ISIS 2.0 increases global risk by a hundredfold while raising new questions. When ISIS is defeated in Syria, will they aim to acquire another State or maintain destabilized regional pockets that keep the West in a perpetual, low-grade war? Further, as we prepare to tackle these new challenges, are we considering the long-term implications, as well as what this will mean to societies in 2035, and to government agencies or the military from 2018 onwards?

AI and the impact of ISIS, terror and trafficking groups leveraging Cryptocurrency to bypass traditional black market terror financing operations need to be assessed. As the cost of AI and Bots has reduced with time—automated terror via AI and crypto-funding of terror activities raises additional risk.

Our long-term goals should be to develop integrated protocols and SOPs that have measurable KPIs to counter ISIS and evaluate online social sentiment. We also need to be cognizant of the risks that Crypto, social media and cyber pose in a landscape where we will be using cyber to fight Social Media Terrorism and Crypto Terror. We also need to focus on improving information sharing between US military services, IC, government agencies, Nations, and the business community.

The intersection of these areas also present a further risk as technology moves into AR/VR and touchable Holograms—the threat of Terrorism 4.0 is only a few years out. ISIS has shown us the threat within the real-time, social media environment. The time to tackle that threat is now. 🛡️

THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆

Cyberspace Operations Collateral Damage – Reality or Misconception?

Giorgio Bertoli, CISSP
Dr. Lisa Marvel

ABSTRACT

Practically all military actions have the potential to result in undesirable collateral damage. Laws and international treaties mandate the minimization of civilian casualties and damage to civilian property. To enforce this, the military developed methods and tools to help predict the collateral damage that may result from the employment of specific weapon systems under various conditions. These processes have been refined over time, and are now very effective for the planning of kinetic operations. The emergence of cyberspace as an operational domain, however, adds new complexities. Evaluating the overall impact of a cyberspace weapon is less intuitive and more multifaceted to predict. Cyberspace capabilities have inherent differences in their behavior and employment that require additional study and scrutiny. These complexities, however, have been misconstrued and mythicized to the point where the perceived damage that can result from the utilization of any cyberspace tool is often greatly exaggerated. When decomposed, as part of a holistic collateral damage taxonomy, the processes for quantifying the undesirable effects that may result from the employment of many types of cyberspace weapons is not that much different than from their kinetic counterparts.

Keywords—Collateral Damage, Cyberspace Operations

I. INTRODUCTION

Imagine we have received intelligence confirming that a group of insurgents has established an operations center in the midst of a busy residential area. From within this base of operations, the enemy has created a recruiting campaign leveraging social media. They have also gathered a team of hackers to eavesdrop on local US Army assets and to spread misinformation. The cell is small but effective, and their work is directly impacting the fight. We know we must strike—but how?

© 2017 Giorgio Bertoli, Dr. Lisa Marvel



Mr. Giorgio Bertoli, CISSP works for the U.S. Army Intelligence and Information Warfare Directorate (I2WD), Communications-Electronics Research Development and Engineering Center (CERDEC), US Army Research Development and Engineering Command (RDECOM), as Senior Scientific Technology Manager (SSTM) of Offensive Cyber Technologies.

With 22 years of federal service, Mr. Bertoli has extensive government experience in Cyber, Electronic Warfare, and military tactics. Mr. Bertoli's research areas include the development of advanced Electronic Warfare (EW), Computer Network Operations (CNO), Cyber, and Quick Reaction Capability (QRC) technologies.

Mr. Bertoli has a Bachelor's and Master's Degree in Electrical Engineering from the New Jersey Institute of Technology, and a second Master's Degree in Computer Science from the University of Massachusetts Amherst. Mr. Bertoli is a Certified Information Systems Security Profession (CISSP). During his 6.5 year Military career, Mr. Bertoli served as a combat Engineer and deployed as part of Operation Desert Shield and Operation Desert Storm.

Within a two-block radius are a dozen houses, six businesses, a hospital, a house of worship and an elementary school. Our Soldiers work to pull together a plan. They know they can use traditional weapons to strike with precision, and they can accurately predict the risk to local civilian populations and property. They discuss the possibility of a cyber offensive, which would reduce risk to the civilian population and minimize the threat to an already precarious environment, but commanders are uncertain of potential unintended outcomes and are limited in their ability to quantify the likelihood of related 2nd and 3rd order effects. Ultimately, they choose the kinetic weapon to engage the target and accept the known risks associated with this course of action.

The ability to accurately predict all potential consequences (both intended and unintended) often govern our decisions on what amount and type of military force to employ. Over the past century, the military has developed effective processes and metrics to quantify the risk associated with the use of kinetic weapons. Now, the advent of cyberspace warfare is providing new challenges where effects are less tangible and more difficult to define in term of "blast radius" and "probability of hit". The resulting uncertainty has over-amplified the perceived risks associated with the employment of cyberspace capabilities.

The execution of any action has associated consequences. Most often, these consequences are intended, and the reason the action was undertaken. Sometimes, however, actions can have other unintended, and often undesirable, effects. Examples of this are easy to find, whether as side effects of certain medications, car accidents as a byproduct of driving, or more relevantly, civilian casualties due to military conflict. We designate all such negative events that can result from a specific action as un-



Dr. Lisa Marvel until her recent retirement, was a researcher with the U.S. Army Research Laboratory (ARL) at Aberdeen Proving Ground, Maryland. Her research interests include coding, communications and cybersecurity. She received her B.S.E.E. degree from the University of Pittsburgh in 1992 and the M.S. and Ph.D. degree in electrical engineering from the University of Delaware in 1996 and 1999, respectively. Lisa holds an Affiliated Faculty position with the Computer and Information Sciences Department at the University of Delaware. Additionally, she was the Agility Lead for the ARL Cyber Security Collaborative Research Alliance (ARL Cyber CRA).

intended consequences. Collateral damage is then a subset of these unintended consequences that can occur as a result of intentionally destructive actions; often used in a military context.

Given most actions can have the potential for unintended results, the mechanism we use to decide if an action is worth taking involves evaluating the associated risk of all potential outcomes. In most cases, for mundane everyday actions, this is a simple process that we perform almost intuitively based on experience. For more complex situations (e.g. project management), a methodology for the evaluation of risk, based on the likelihood that a specific undesirable event will occur, and its associated severity, is commonly used. [1] To ensure accuracy, it is essential that all key factors that can lead to unintended consequences are considered. The root causes of collateral damage can be categorized into a generic higher order taxonomy. This taxonomy can then serve as a useful model for the evaluation of the overall collateral damage risk associated with a specific destructive action.

II. BACKGROUND AND MOTIVATION

In 2011, the Department of Defense identified cyberspace as an operational domain [2]. This designation effectively placed this new, virtual, man-made environment on par with the more tangible physical operational domains of land, air, sea, and space. The need for the US to defend and project power within and through this domain at various echelons have since been codified in emerging doctrine [2][3] and discussed in multiple articles [4][5].

International law and treaties govern military operations in any domain. These laws explicitly state “in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects” [6]. This legal require-

ment to minimize collateral damage must also be applied to cyberspace operations. This, however, is not a simple extension from the more familiar physical domains. Cyberspace transcends geographical boundaries. Execution of activities within it are near the speed of light. It is, in many ways, an intangible battlespace in which executed effects are not governed by the laws of physics and, as a result, are hard to predict [7][8]. Given these challenges, it is difficult to measure the risk associated with the execution of an offensive cyberspace capability and to estimate the amount of collateral damage that it may cause. Evidence that our inability to quantify this risk has impeded the employment of cyberspace capabilities has been publicly reported [9], and will undoubtedly continue to limit our capacity to operate within this new domain if not overcome.

There is a prevalent misconception that all cyberspace effects are analogous to biological agents, in that, once released they will propagate and infect others with impunity^[1], lending to the belief that they are incapable of precision targeting. This is simply not true in many cases. In addition, there is an inclination for applying a higher standard of fidelity to cyberspace capabilities. Neil Rowe, in his work “The Ethics of Cyberweapons in Warfare,” [8] provides one such example.

Cyber warfare does not target military personnel directly but only their software and data. But usually, cyberattacks will be effective against any computer with the same type of vulnerable software. Military organizations use mostly software that is also used by civilians. So civilian computers could also suffer from military cyberattacks; in fact, they are usually more vulnerable because their countermeasures are not as good.

While this is certainly a true statement, it is hardly unique to cyberspace capabilities. Could you not also claim that a bullet is equally effective against both military and civilian personnel? And, that civilians are actually at greater risk as they lack training, body armor and other protective mechanisms afforded to the military?

The highly technical nature of cyberspace, coupled with overzealous rhetoric by the media and other proponents [10][11][12], has resulted in an exaggeration, or often, a downright misrepresentation of the actual risk [13][14][15]. The potential for an offensive cyberspace weapon to cause collateral damage is undeniable; however, while such capabilities are different from their kinetic counterparts, they are not mystical. Many can be well controlled in their function and behavior.

In the rest of this article, we define a general taxonomy for the root causes of collateral damage and compare cyberspace weapons to their more traditional counterparts. We will demonstrate that, in many cases, they are not significantly different, and as such, existing risk assessment approaches can be applied.

^[1] The term “computer virus” was coined in 1984 by Frederik Cohen to describe the operation of self-replicating computer programs synonymous to a biological “infection” because of the conceptual similarities in their ability to infect others.

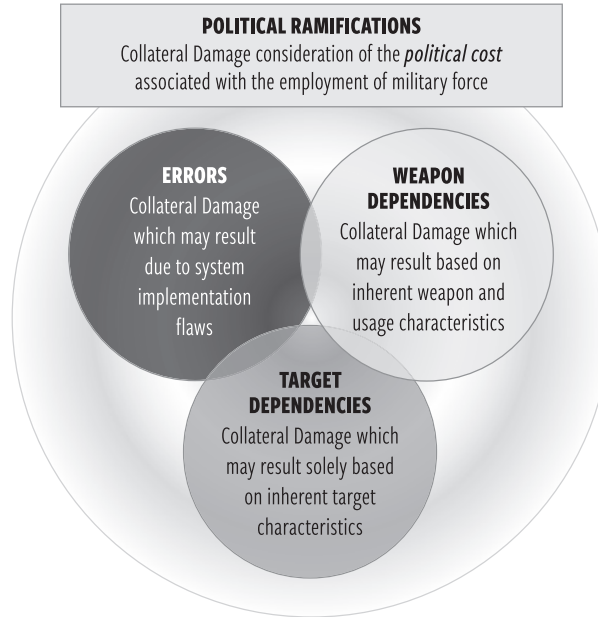


Figure 1. Generic Collateral Damage Taxonomy

III. GENERIC COLLATERAL DAMAGE TAXONOMY

In general, collateral damage may be categorized into four distinct contributing factors [7][8] (Fig 1).

- ◆ *Errors (E)*: Reflect the collateral damage that may result due to the presence of design or implementation flaws that leads to unintended system performance.
- ◆ *Target Specific Dependencies (TD)*: Reflect the collateral damage that may result solely based on properties and dependencies inherent to the target system.
- ◆ *Weapon Specific Dependencies (WD)*: Represents the collateral damage that may result solely based on the intrinsic properties, execution behavior, or employment methodology of the weapon system.
- ◆ *Political Ramifications (P)*: Encompass the less tangible political and moral aspects of collateral damage to include considerations of public perception and international backlash, gain/loss equities, as well as ethical national principles.

When combined (Eq. 1), these individual aspects of collateral damage will provide the total collateral damage risk (CDR) associated with a specific action, within the context of the environment in which it is executed.

$$CDR = F(R(E), R(TD), R(WD), R(P)) \quad (1)$$

Where each sub-risk element $R(\dots)$ can be computed using the standard “Probability of Occurrence Vs Impact” risk model.

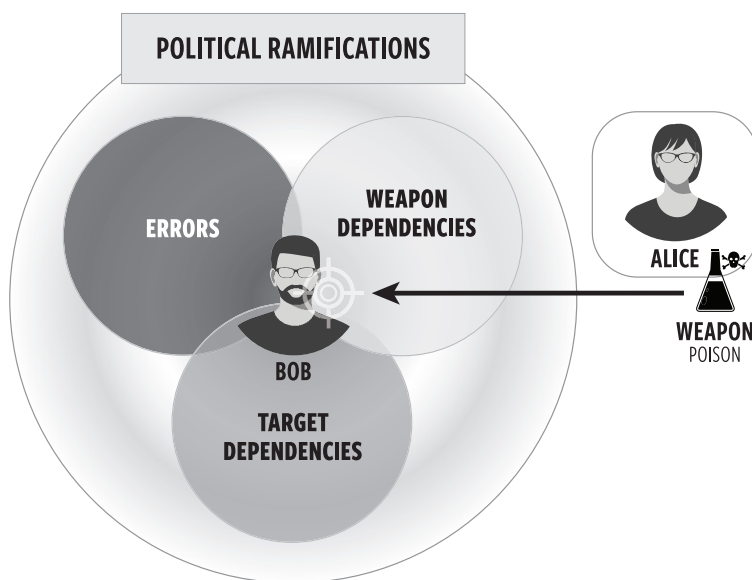


Figure 2. Taxonomy Case Study

IV. SIMPLE ILLUSTRATIVE EXAMPLE

To better illustrate this proposed taxonomy, let us apply it to an intuitive example. In this simple use case (figure 2), Alice (our weapon operator) wishes to poison (the weapon system) Bob (her target).

Given this simple construct, we can consider how each of the four categories within the described risk taxonomy would apply.

- ◆ *Errors (E)*: The poison could potentially have a flaw. For instance, it may take a much longer time for Bob to die than desired. During this time, others who come in contact with Bob's bodily fluids could also be poisoned themselves. This is clearly collateral damage due to an error or malfunction in the weapon system.
- ◆ *Target Specific Dependencies*: What if Bob was a prominent medical researcher? Perhaps Bob was on the cusp of a revolutionary discovery for a new vaccine. As a result of his death, this work can no longer continue and many more people will die from the disease he would have cured. You will note, that this form of collateral damage is completely independent of the weapon system employed. This same outcome would have occurred if Bob had died naturally or by some other means.
- ◆ *Weapon Specific Dependencies*: Given this poison must be ingested; Alice decides to contaminate the water supply of the town Bob resides in. As a result, the poison will affect a lot more people beside Bob. This type of collateral damage is only dependent on the weapon system. In this example, specifically in the way it was employed.

- ◆ *Political Ramifications:* This last category must take into account other intangible considerations. What will be the international backlash to Bob's death? What if the poison is discovered as a result of an autopsy? Could something in the formulation provide attribution of its creator? Could an antidote now be crafted to prevent Alice from using this poison again? Or worse, could the poison be reverse engineered and then used against others?

V. OFFENSIVE CYBERSPACE CAPABILITY COMPARISON

With a clear understanding of the presented collateral damage taxonomy, we can now address what additional considerations, unique to cyberspace weapons, must be made.

- ◆ *Errors:* Historically, programming errors within computer exploits have been a significant source of unintentional disruptive behavior, which in turn directly led to or exacerbated the amount of damage that resulted. It is important to note, however, that exploits "released in the wild" are often developed by relatively unsophisticated programmers who likely have little concern for the collateral damage that may result. This is not the case for professionally developed capabilities. The potential for design or implementation flaws are factors that must be considered by all weapons system. Minimizing this particular source of collateral damage is best done through the implementation of sound development, testing, and validation procedures; guidelines that are already included as part of existing acquisition processes. When such procedures are followed, this risk category should not be any different when applied to cyberspace weapons^[2].
- ◆ *Target Specific Dependencies:* It may be the case that the execution of a cyberspace effect, which significantly impacts the targeted system, will cause additional unintended damage based on the dependent processes that system controls. A classic example is a hypothetical attack targeting a Programmable Logic Controller (PLC) that manages some step of a greater physical process (e.g., a waste treatment plant, or a manufacturing facility). Altering or limiting the functionality of such a device may disrupt the overall physical process it supports with potentially catastrophic consequences that are both difficult to predict, and that can cascade to cause additional unintended events to occur^[3]. Such collateral damage, however, is not a function of the attack mechanisms used^[4], but rather is directly related to the target system and the processes it controls^[5]. Calculating this aspect of collateral damage must be

^[3] As an example, imagine a Cyberattack is conducted against a power generation plant. The exploit shuts down a specific component resulting in a power outage. This (especially if ongoing for extended periods of time) may have significant 2nd and 3rd order ripple effects. Other power plants may also be impacted due to the additional power draw that results as they try to compensate. If streetlights no longer function, traffic conditions can quickly become gridlocked. Local businesses can no longer utilize Point of Sale systems or process credit card payments, which will, in turn, result in financial losses and possibly civil unrest, and so forth.

^[4] The same collateral damage would result regardless of the cause for the malfunction (for instance, a mechanical failure or a kinetic strike).

^[5] It can be argued, that for this aspect of collateral damage, non-kinetic engagement options have a distinct advantage over more traditional kinetic warfare since any damage caused, to include any potential collateral damage, may be more readily reversed [18].

performed from the perspective of the target system and requires an in depth understanding of all its functions and dependencies.

- ◆ *Weapon Specific Dependencies:* Collateral damage can result from the uncontrolled execution of a cyberspace capability. By its inherent design, cyberspace transcends physical boundaries, such as geographical proximity, and can operate on varied time scales (both extremely small and extremely long). As a result, depending on its design, the release of a software application (malicious or otherwise) within this environment may be difficult to restrict its distribution or “spread” can be hard to control or predict. Consequently, a cyberspace effect that is employed against a specific target system may also unintentionally or indiscriminately impact other systems. This is a unique aspect of some cyberspace weapons when compared to their kinetic counterpart.
- ◆ *Political Ramifications:* The employment of a cyberspace weapon (with well-defined behavior) will not significantly change this last risk consideration. One exception will be in the determination of equities. Just as in our simple use case, cyberspace effects are often perishable, and their usefulness is significantly decreased once discovered. Also, they may be reverse engineered and repurposed for more nefarious usage by a third party.

In summary, as per table 1, it can be shown that deriving the overall collateral damage risk associated with a cyberspace capability is not markedly different from those of more conventional weapon system.

Collateral Damage Category	Kinetic Weapon System Possible Collateral Damage	Cyber Weapon System Collateral Damage Considerations
ERRORS	Errors can lead to malfunctions that results in civilian casualties property	Errors can lead to malfunctions that results in civilian casualties property
TARGET SPECIFIC DEPENDENCIES	Processes governed by the target system may fail resulting in cascading collateral damage effects.	Processes governed by the target system may fail resulting in cascading collateral damage effects. However, they may be easier to reverse or recover from.
WEAPON SPECIFIC DEPENDENCIES	Weapons have well defined targeting probability and blast radius based on well understood physical and empirical models.	Some cyber weapons may be capable of propagating outside the bounds of the intended target system with harder to predict limitations.
POLITICAL RAMIFICATIONS	Traditional use of force and proportional response considerations	Same plus additional concerns regarding potential loss of weapon effectiveness and possible 3rd party repurposing.

Table 1: Collateral damage consideration comparison between kinetic and cyber weapons

Within this taxonomy, only the “Weapon Specific Dependencies” attribute is significantly unique to cyberspace operations. To identify the risk associated with this specific cause of collateral damage, we must quantify what undesired consequences may occur as a result of the emergent/uncontrolled behavior inherent within a cyberspace weapon’s design. While this is sometimes difficult, methods for bounding the amount of damage that can result have been studied [16]. Furthermore, many cyber capabilities significantly limit (or altogether do not possess) the ability to spread beyond the target system, thus negating this risk altogether. It is this facet of “cyber” collateral damage that is overemphasized and often mistakenly intertwined with other risk factors, which are beyond the weapon system’s control, that contribute to the misconception that cyberspace capabilities cannot be safely employed in support of military operations [17].

VI. CONCLUSION

As with any military weapon system, consideration for the collateral damage that may occur based on the employment of offensive cyberspace capabilities must be assessed and quantified. Cyberspace effects and tools have unique operational characteristics that present specific challenges for the determination of collateral damage risk. These challenges, however, are not insurmountable. As described, most of the core contributing factors leading to collateral damage are independent of the weapon system used and therefore can leverage already established risk determination processes. Additional work conducted by the Communication-Electronics Research Development and Engineering Center (CERDEC) and Army Research laboratory (ARL) has built upon the taxonomy presented in this paper to develop a methodology for the quantification of the collateral damage potential associated with a specific computer exploit^[6][16]. The non-intuitive and highly complex nature of the cyberspace domain has resulted in an overinflated perception of the risk associated with the employment of cyberspace capabilities. In many cases, the use of non-kinetic cyber effects can be well defined and more desirable than their kinetic counterpart. 🛡️

^[6] Please contact the authors of this paper for additional information.

NOTES

1. MITRE, "System Engineering Guide: risk impact assessment and prioritization," MITRE, [Online]. Available: <https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization>, Accessed June 30, 2016.
2. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 2011.
3. Department of Defense, Joint Publication 3-12(R) - Cyberspace Operations, US Department of Defense, 2013.
4. M. Leed, "Offensive Cyber Capabilities at the Operational Level," Center for Strategic & International Studies, 2013.
5. J. K. Sandborn, "Cyber Steps up its role on the battlefield," *Army Times*, Aug 25, 2014.
6. Department of Defense, Law of War Manual, Washington, DC: OFFICE OF GENERAL COUNSEL, 2015.
7. P. Lin, F. Allhoff and N. Rowe, "Computing Ethics, War 2.0: Cyberweapons and Ethics," *Communications of the ACM*, vol. 55, no. 3, 24-26, 2012.
8. N. C. Rowe, "The Ethics of Cyberweapons in Warfare," *International Journal of Cyberethics*, vol. 1, no. 1, 2009.
9. J. Markoff and T. Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times*, August 2, 2009.
10. T. Capaccio, "Cyber-Armageddon Less Likely Than Predicted, Clapper Says," 25 2 2015. [Online]. Available: <http://www.bloomberg.com/news/articles/2015-02-26/cyber-armageddon-less-likely-than-smaller-attacks-clapper-says>.
11. B. Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated," CNN.com, 7 7 2010. [Online]. Available: <http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/>.
12. T. Payton, "Cyberwarfare - Fact or Fiction?," 27 8 2010. [Online]. Available: <http://www.infosecisland.com/blogview/6845-Cyberwarfare-Fact-or-Fiction.html>.
13. T. E. Smith, "Cyber Warfare: A Misrepresentation of the True Cyber Threat," *American Intelligence Journal*, vol. 31, no. 1, 82-85, 2013.
14. S. Lawson, "Beyond Cyber-Doom," Mercatus Center, George Mason University, 2011.
15. K. Fink, J. Jordan and J. Wells, "Considerations for Offensive Cyberspace Operations," *Military Review*, no. May-June, 4-11, 2014.
16. G. Bertoli and L. Marvel, "Collateral Effect Potential Metric for Computer Exploits," Available from giorgio.bertoli.civ@mail.mil, Aberdeen Proving Ground, MD, 2016.
17. C. B. A. Metcalf, "Tactical Cyber: How to Move Forward," *Small Wars Journal*, 2014.
18. N. C. Rowe, "Towards Reversible Cyberattacks," in *Proceedings of the 9th European Conference on Information Warfare Security*, Thessaloniki, Greece, 2010.

The Cyber Domain

Dr. Glenn Alexander Crowther

ABSTRACT

Both the Department of Defense (DoD) and the North Atlantic Treaty Organization (NATO) have declared that cyber is a “domain”, co-equal with air, land, and sea. DoD also recognizes space as a domain. Merriam-Webster defines a domain as a sphere of knowledge, influence, or activity.^[1] Although DoD does not define “domain”, it does define cyberspace as “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”^[2] No one has yet proposed what the cyber domain is, where militaries should be operating in cyberspace, and what missions’ militaries should be doing in cyberspace. This article identifies what DoD says their missions are in cyberspace and discusses what areas are appropriate for military operations in cyberspace. Additionally, it argues that militaries must be very careful about what missions they accept in cyberspace, and must circumscribe their forays into cyberspace lest they are overwhelmed by the sheer scope of the domain.

CIRCUMSCRIBING THE MILITARY CYBER DOMAIN

The military must limit its activities within cyberspace. Just as modern megacities could absorb entire armies, the Internet would swallow the entire cyber capability of not only the DoD but also the capabilities of partners and Allies. It is therefore important to choose how to circumscribe military cyber activities within cyberspace. This is not meant to limit where military cyber units may operate, but rather to limit what functions military cyber resources participate in, thereby preserving cyber capabilities for mission requirements rather than frittering cyber capabilities pursuing wills-o’-the-wisp through cyberspace.

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



Dr. Glenn Alexander Crowther is the Senior Research Fellow for NATO/Europe and Cyber Policy in the Institute for National Strategic Studies (INSS) at NDU. His work at the strategic level includes tours at the Army Staff, the Joint Staff J5, and as a Research Professor at Strategic Studies Institute. He was personally selected to be a Counterterrorism Advisor for the US Ambassador to Iraq, a Political Advisor for the MNC-I Commander, and a Special Assistant for the SACEUR. He has published in a variety of formats and locations, has experience teaching at the graduate level and has extensive experience as a public speaker in a wide variety of locations. Alex has a BA in International Relations from Tufts, an MS in International Relations from Troy University, and a Ph.D. in International Development from Tulane. He was also an International Security Studies Fellow at the Fletcher School of Law & Diplomacy.

In the United States, 90% of cyber activity is in private hands.^[3] In Europe, the statistics are similar.^[4] Thus, the military should not be operating within 90% of the Internet unless it pertains to one of the mission sets that this article identifies as appropriate for military participation. When pursuing these mission sets, the military can go where they need to in cyberspace, however, they should avoid entering into most private and commercial cyber interactions, not only for the sake of privacy and limitations on the use of military instruments (such as *posse comitatus*, the 1877 U.S. law that proscribes military activities inside U.S. territory) but also to retain freedom of maneuver. As an example, military cyber operators should not be concerned with PayPal interactions with Amazon, unless the person initiating the payments is involved in something that would make them the target of intelligence operations.

DoD has three primary cyber missions: Defend DoD networks, systems, and information; Defend the US homeland and US national interests against cyberattacks of significant consequence; and Provide cyber support to military operational and contingency plans.^[5] In order to perform those missions, reports estimate that DoD has a “cyber workforce of more than 160,000 military and civilian personnel”: 3777 for defensive operations, 145,457 for operation and maintenance and 13,910 working on information assurance. Another 6200 in the Cyber Mission Force adds up to 169,344 cyber operators.^[6] Although this sounds like a great many resources for the Department to wield in cyberspace, this number represents a requirement for the military to accept a circumscribed mission set because of finite resources. Although eventually everyone in DoD will eventually be involved in cyber-enabled operations, they will not be performing defensive and offensive cyber operations. This points to the need to be parsimonious in the allocation of cyber resources.

Just like the U.S. Army could be absorbed by future megacities like Lagos, Nigeria^[7], the vast and growing expanse of the Internet would swallow the DoD cyber workforce, whether it be 170,000 or 1.7 million workers. There is pressure on DoD to participate in cyber operations outside of their three stated mission sets. If national security policy makers insist that DoD should expand their cyber mission set, and should DoD accept the new, expanded missions, then DoD would court disaster.

U.S. joint doctrine recognizes the nine principles of war: objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, and simplicity.^[8] Not circumscribing military missions in cyberspace violates at least three principles: mass, economy of force, and simplicity.

An expanded mission set might include helping to protect Internet users in the US. In 2016, there were 287 million Internet users in the US.^[9] If there are 170,000 cyber warriors helping to protect US persons using the Internet would mean one DoD cybernaut is helping almost 1700 internet users. If this example is too extreme, some people believe that DoD assets could help businesses. As large businesses typically have some cybersecurity, small businesses would need the most help. As there were 28.8 million small businesses in the United States in 2016^[10], there would be one cyberwarrior helping 170 small businesses. These two examples should suffice to prove that DoD does not possess the resources to help the private sector.

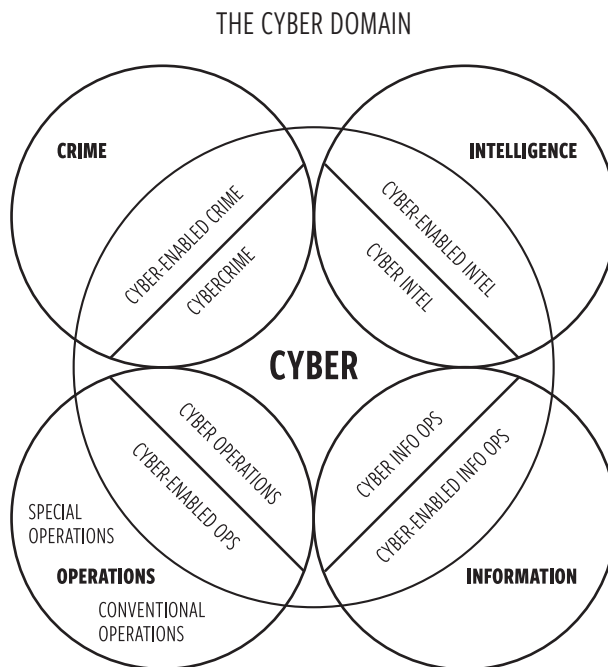


Figure 1. The Military Cyber Domain

Where Should the Military Operate in Cyberspace?

If the military should not be supporting the private sector, what should they be doing in cyberspace? There are four sets of cyberspace activities that pertain to the military: intelligence, information, crime and military operations.^[11] Militaries participate in intelligence operations, conduct information operations, conduct and support conventional and special operations, and respond to a limited subset of crime. Together these four areas make up the military cyber domain.

Although the military has equities in all of these areas, the only area that the military predominates in is the military operations portion. There are, however, intelligence, information and criminal activities that involve the military. Figure 1 illustrates the Military Cyber Domain. In any of these four fields, there is a spectrum of activity, from the conventional activity to cyber-enabled activity to cyber activity in that field to purely cyber operations. The remainder of this paper examines each of the four areas that are appropriate for military operations.

Cyber Operations

In the center are pure cyber operations that the Department would be doing anyway: Information and Communications Technology (ICT), Network Operations, and Defensive Cyber Operations (DCO). This is the manifestation of the first DoD cyber mission: to defend DoD networks, systems, and information.

The first mission set under “cyber operations” is ICT.

ICT refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. Although ICT is often considered an extended synonym for information technology (IT), its scope is broader. ICT has more recently been used to describe the convergence of several technologies and the use of common transmission lines carrying very diverse data and communication types and formats.^[12]

Information and Communications Technology, therefore, provides the backbone of all military activities. Can anyone imagine running a modern military without telecommunications and diverse data and communications types? This includes all of the communications devices including computers and telephones. The DoD Chief Information Officer (CIO) is the Principal Staff Assistant and senior advisor to the Secretary of Defense for information technology (including national security systems and defense business systems), information resources management and efficiencies. As such, the CIO is responsible for ICT in the Department, and is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2).^[13]

Network operations is the next mission set under “cyber operations.” The Defense Information Systems Agency (DISA) is overall responsible and provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations.^[14] The global DoD network is called the Department of Defense Information Network (DODIN). DISA operates DODIN while each of the services has their own portion of DODIN such as the U.S. Army Network Enterprise Technology Command (NETCOM) and the Air Force Information Network (AFIN). DISA also provides direct telecommunications and IT support to the president, vice president, their staff, and the U.S. Secret Service through the White House Communications Agency.^[15]

Defensive Cyber Operations is the last mission under “cyber operations.” According to the DOD Joint Publication 3-12 (R), Cyberspace Operations, “DCO are Cyberspace Operations (CO) intended to defend DOD or other friendly cyberspace ... (and) are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.”^[16]

These three cyber operations areas underlie all military functions. Although it is possible to perform other military functions (such as fires) without ICT, network operations, and DCO, it has become more and more difficult to do so. The facts that the U.S. Naval Academy have had to add a class to teach Midshipmen to navigate with sextants^[17] and the U.S. Army Infantry School has realized the importance of teaching their Infantry Officers to use a map and compass^[18] illustrates how rare it is for operations to do without these three cyber functions.

The Military and Cyber Intelligence

Militaries have participated in intelligence operations as long as there have been organized forces. Sun Tzu wrote about the use of intelligence by the military.^[19] The modern manifestation of US national intelligence demonstrates this strongly as the US Intelligence Community admits that no less than eight of their 17 members belong to DoD.^[20] Therefore, it makes sense that the military should be operating in cyberspace as part of their intelligence mission.

Normal intelligence operations would be the traditional approach to intelligence before the advent of cyberspace: stealing secrets, developing sources, etc. As modern societies become more informationized, fewer intelligence operations will occur without technology. Infiltrating terrorist cells and other traditional methods of gathering the data that eventually becomes intelligence will continue to be important in areas that are not integrated into the global information system, such as remoter areas in the Middle East, Central Asia, and Africa. Traditional spycraft will also be required to infiltrate organizations that specifically adopt approaches to minimize or avoid vulnerability to advanced intelligence-gathering techniques (such as signals intelligence), such as al-Qaeda and Daesh.

THE CYBER DOMAIN: INTELLIGENCE

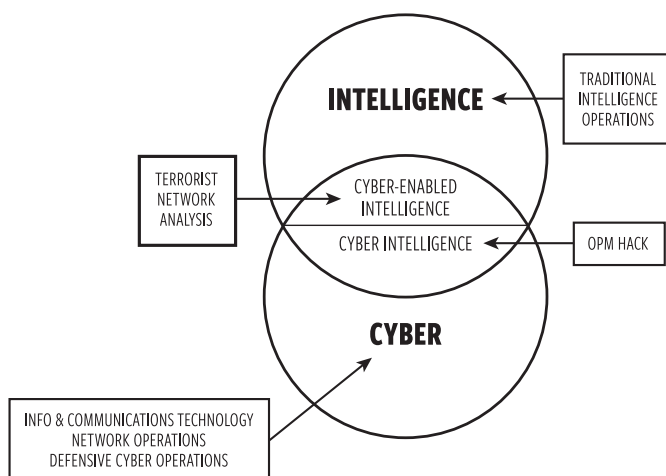


Figure 2. Relationship between Cyber and Intelligence

Cyber-enabled intelligence operations would use cyber capabilities in support of intelligence operations. One example would be terrorist network analysis using data that had been gathered by traditional intelligence means such as human intelligence. More and more of these intelligence operations are becoming cyber-enabled intelligence. In the long run, almost all traditional intelligence operations will be cyber-enabled intelligence operations as collection and analysis methods are significantly improved through the use of nanotechnology and artificial intelligence.

Cyber intelligence operations would be where the intelligence operation occurs entirely in cyberspace. Examples include the 2012 operation by Chinese hackers that penetrated Indian Navy computers and compromised sensitive information^[21] or the 2015 hack on the US Office of Personnel Management, where the personnel records for at least 22.1 million people were “affected by cyber intrusions that U.S. officials have privately said were traced to the Chinese government”.^[22] As more and more records are maintained electronically, more intelligence operations will be executed entirely within cyberspace. Although pure cyber intelligence operations will increase in number, there will always be a need for traditional intelligence operations until human beings are no longer involved.

The Military and Cyber Crime

At first blush, it makes no sense at all that a military would be involved in any crime protection, much less cybercrime. In the United States, the Department of Justice has the lead for cybercrimes while the Department of Homeland Security has responsibility for cybercrimes under their jurisdiction.^[23] However, the ubiquity of cybercrime and the specific targeting of defense-related industrial and personnel information requires that militaries at least pay attention to cybercrime.

The Defense Cyber Crime Center (DC3) serves as the operational focal point for the Defense Industrial Base (DIB) Cybersecurity Program. They provide digital forensics and multimedia (D/MM) lab services, cyber technical training, technical solutions development, and cyber analytics for the following DoD mission areas: cyber security (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT).^[24] DC3 also leads efforts to deal with any cybercrime that involves DoD personnel.

Their involvement in the DIB is particularly important as the US depends on technological advantages on the battlefield, while adversaries seek to steal the technology and sell it, use it themselves, or figure out how to mitigate effects on the battlefield. An excellent example of that is the theft of C-17 plans, where hackers stole 630,000 files from Boeing's system, totaling some 65 gigabytes of data, and volumes of data on the Lockheed Martin F-35 and F-22.^[25] The DIB Cybersecurity (CS) Program DoD is designed to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems. It is a public-private cybersecurity partnership designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness. Under the DIB CS Program, DoD and DIB participants share unclassified and classified cyber threat information.^[26]

Conventional criminal operations would be an old-school crime, such as entering a bank with a pistol and a bag to steal money. As long as there is cash and people are vulnerable to crimes such as kidnapping, these crimes will continue. Cyber-enabled criminal operations fuse technology and crime. One example is ATM-skimming, where criminals use hidden electronics to steal the personal information stored on your card and record your PIN number. They then later access your account.^[27] Keylogging is a similar cyber-enabled crime, where hackers gather account information via the technique of recording keystrokes and then later using the information to log into other people's accounts. Pure cybercrime would be a criminal operation that occurs wholly in cyberspace, such as the use of the SWIFT system to steal \$81 million from the Bank of Bangladesh.^[28]

THE CYBER DOMAIN: CRIME

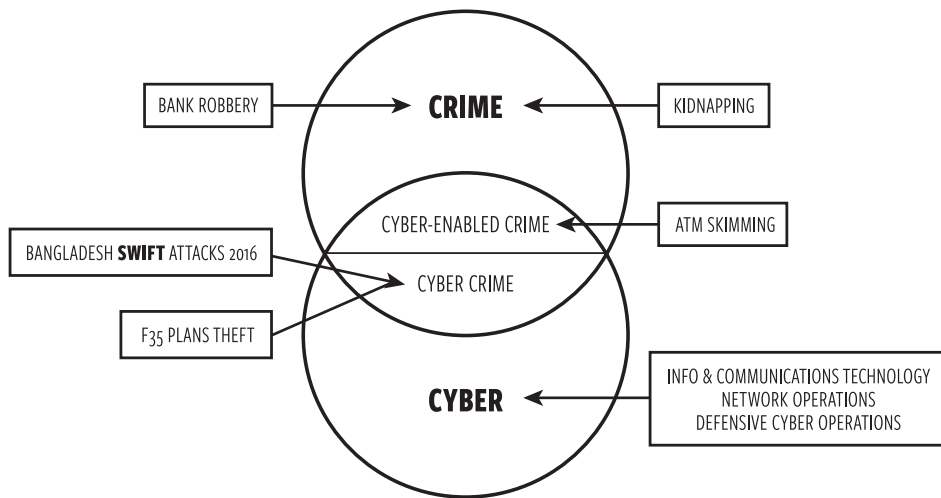


Figure 3. Relationship between Cyber and Crime

One major gain for the United States and global allies and partners is the codification of cybercrime as the equivalent of non-cyber or traditional crime. Robbing a bank at gunpoint is now recognized to be the same as using cyber means to steal money from a bank. Russia and China had previously felt that cyberspace was like the Wild West, where the law did not prevail.^[29] During the 2015 meetings of the UN Group of Government Experts, China and Russia both joined the rest of the participants in agreeing that international law does run writ in cyberspace. That means that both intelligence and crime in cyberspace are covered by extant law that deals with the two subjects. The U.S. Congress has an ongoing effort to update laws within Title 50 (War and National Defense) and Title 18 (Crimes and Criminal Procedure) of the United States Code to ensure that cybercrimes are captured in U.S. law.^[30]

The Military and Information Operations

Militaries have been using operations in the information environment to shape cognition for the entire history of warfare. Sun Tzu refers to all warfare being based on deception, a form of information operations. Information operations^[31] featured strongly during the Cold War and have returned to importance as a global China and a resurgent Russia conceptualize the informationization of modern societies.^[32] Russia has returned to the aggressive use of Active Measures or Political Warfare against NATO Allies and partners, in particular, their neighbors over who the Government of Russia seeks to reestablish hegemony.^[33] China has developed the concept of the “Three Warfares” which includes lawfare, media warfare, and propaganda warfare.^[34] All three have strong connections to the use of information.

THE CYBER DOMAIN: INFORMATION

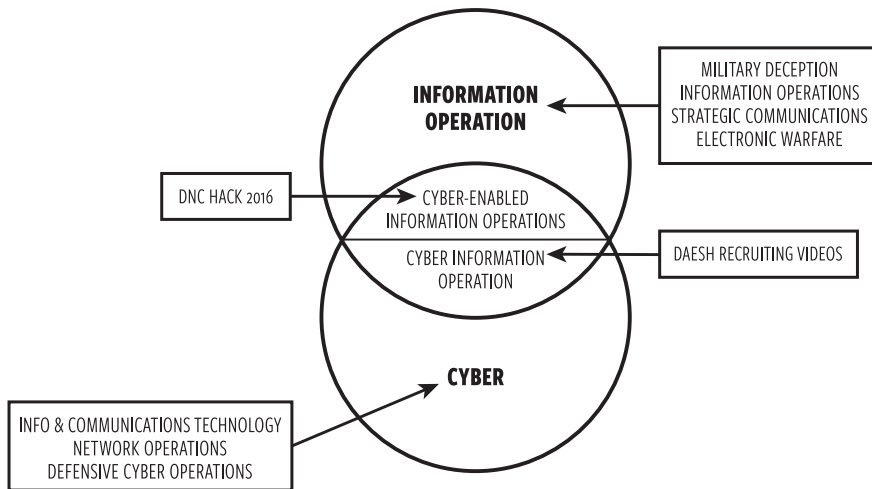


Figure 4. Relationship between Cyber and Information

In addition to the Three Warfares, China has made advances in conceptualizing “strategic information war”. This concept “refers to the use of information and information technology in the political, economic, (science & technology), diplomatic, cultural, and military arenas to secure information advantage. In this broad sense, information war spans military and civilian spheres, peacetime and wartime, and has a global nature.”^[35] Although there are a variety of names for the Russian approach, the most accurate appears to be “new generation warfare” which “is manifested in five component elements: political subversion, proxy sanctuary, intervention, coercive deterrence and negotiated manipulation.”^[36] Together these two approaches provide a significant threat to the United States, NATO Allies and like-minded partners around the world. This means that we all need to be competing in the information space. Information competition is so important that the Chairman of the Joint Chiefs of Staff recently designated “information” to be a joint function, co-equal with the existing joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.^[37]

The military has five functions that partially exist in the information environment and seven that exist entirely within the environment: Information Operations (IO), Military Deception, Psychological Operations (PSYOPs, also known as Military Information Support Operations or MISO), Public Affairs, and Strategic Communications are entirely within the environment. Communications & Signals, Cyber, Electronic Warfare (EW), Intelligence, Space operations and Operations Security (OPSEC) exist partially within. Physical operations also have an information effect, as when a US Army unit goes to a firing range in eastern Poland. All of these functions are legitimate military operations within cyberspace.

Conventional information operations are the age-old arts of persuasion. They are sometimes called propaganda (if your opponents are performing the operations), educational material (if your side is doing it) or even advertising via printed text, radio waves or television. Since tribes formed before history was captured, human beings have shaped the cognition of other human beings, both in the ‘in group’ and the ‘out group.’ Even though operations in the information environment have been central to civilization from the beginning, these operations expanded dramatically with the communications revolution inherent in the advent of the telegraph in the 1800s and accelerated with the further evolutionary additions of radio and television.

A new category of operations in the information environment is cyber-enabled information operations, which began with the arrival of the Internet. This takes the form of a traditional operation which uses cyber to magnify the Impact of the operation or to enable the operation itself. The hack of the Democratic National Committee would be an example of a cyber-enabled information operation. The information was obtained through cyber operations (the enabling function) but released via Wikileaks and thence to mainstream media outlets, a more traditional method of disseminating information.

Cyber information operations are a relatively new set of information operations that takes place entirely in cyberspace. An example would include Daesh recruiting videos. Videos are smoothly produced in a variety of languages and are aimed at global youth. As their target audience are digital natives, Daesh builds their products to be consumed as they do other digital materials.^[38]

Countering these types of operations requires that the same techniques be used. As the Carter Center says, “The implementation of preventative community-based policies will equip trusted Islamic scholars and religious leaders with the necessary analysis and digital tools”^[39] meaning that people hoping to counter them must use digital techniques to compete. This makes operations in the information environment a key cyber mission for militaries.

Military Operations and Cyberspace

Military operations can also be cyber-enabled or executed purely in cyberspace. This analytic framework discusses two types of military operations: conventional and special operations.

THE CYBER DOMAIN: OPERATIONS

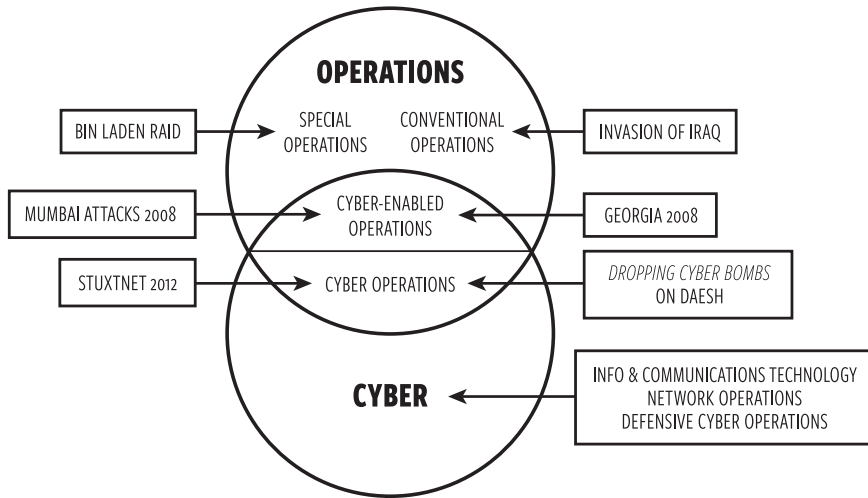


Figure 5. Relationship between Cyber and Operations

Cyber can either enable an operation or can be the operation itself. As such, there are cyber-enabled conventional operations, cyber-enabled special operations, conventional cyber operations and special cyber operations. Cyber-enabled conventional operations happen on a daily basis while almost all special operations (due to the availability of resources) are cyber-enabled. It is probably safe to assume that cyber conventional operations happen frequently and regularly. Cyber special operations, like their kinetic namesake, probably do not occur often.

An example of a conventional or normal military operation would be the invasion of Iraq. An example of a special operation would be the raid to eliminate Osama bin Laden. Although these operations occurred with a minimum of cyber enabling, as time goes on and cyber capabilities suffuse militaries, more and more of these operations will become cyber-enabled. Eventually, all conventional and special operations will become cyber-enabled unless specific counter-cyber operations negate that advantage.

An example of a cyber-enabled conventional military operation would be Russian operations in Georgia in 2008. Although Russia previously conducted purely cyber operations against Estonia in 2007, Georgia was different in that Russia conducted cyber operations against targets in Georgia to affect Georgian command and control in support of conventional military operations on the ground and air.^[40]

An example of a cyber-enabled special operation would be the Mumbai attacks of 2008. Planners used a Go-Pro camera and walked the route so everyone could see videos of their routes during their preparation for the operation. Planners used Google Earth during their planning process. The command and control element monitored Indian social media

and traditional media (such as radio and television) to track the response by Indian security forces and steered the attacking force away from reacting Indian forces, enabling the operation to continue much longer than expected.^[41]

As mentioned, cyber military operations also come in two flavors: conventional and special operations. A conventional cyber operation would be like “dropping cyber bombs on Daesh”. Secretary of Defense Ash Carter explained at an event at US Northern Command that “We’re using these tools to deny the ability of ISIL leadership to command and finance their forces and control their populations; to identify and locate ISIL cyber actors; and to undermine the ability of ISIL recruiters to inspire or direct Homegrown Violent Extremists,”^[42] Although the operations may be classified, mere classification would not be sufficient to label this a special operation. This is a conventional operation in that it does not require special techniques or unique modes of employment, and does not require a covert approach to the operation.

According to Joint Publication 3-05, Special Operations, these operations require:

... unique modes of employment, tactics, techniques, procedures, and equipment. They are often conducted in hostile, denied, or politically and/or diplomatically sensitive environments, and are characterized by one or more of the following: time-sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk...Special operations may differ from conventional operations in degree of strategic, physical, and political and/or diplomatic risk; operational techniques; modes of employment; and dependence on intelligence and indigenous assets.^[43]

A cyber special operation would be the Stuxnet attacks on Iran. It meets many of the criteria for a special operation as defined above. It required unique modes of employment, tactics, techniques, procedures, and equipment. It was conducted in a hostile, denied, or politically and/or diplomatically sensitive environments. It was a low visibility operation characterized by a clandestine or covert nature, as manifested by the fact that no one has yet proved who conducted the operation.

As militaries routinely conduct conventional and special operations, these types of operations involving cyberspace are appropriate for militaries to conduct. All operations will eventually be cyber-enabled while there will be more and distinct cyber operations.

CONCLUSION

Because cyberspace is so large, and so much cyber activity occurs in the private sector, militaries do not have any business operating in most of cyberspace. Although militaries should be able to range anywhere throughout cyberspace to complete appropriate missions, most cyber activity should not involve the military at all.

There are pressures for the military to become more involved in cyberspace. DoD leaders have thus far managed to avoid being dragged into additional areas, mainly by sticking to DoD's three cyber missions: Defend DoD networks, systems, and information; Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and Provide cyber support to military operational and contingency plans. These are legitimate cyber missions for any military. These have been clearly articulated by the U.S. military; however, other militaries probably have not thought this through as they are busy building their cyber forces.

As manifestations of these legitimate cyber missions, there are four areas in cyberspace that are appropriate for the military to operate in: crime, intelligence, information operations and military operations. This article has provided examples of how the military would be involved in all four of these areas. Although military forces are involved in these areas, they are not involved in all operations in these areas (for instance, the Department of Justice handles most cybercrime) but are involved in these areas. This, then, is the circumscribed area that should be called the military cyber domain. Militaries and Alliances like NATO around the world would do well to conceptualize these missions as appropriate for military cyber forces, understand why they should not be performing cyber missions outside of these areas, and inform their political masters that expanding cyber operations away from those four missions risks frittering away cyber combat, which would put at risk the overall mission of the military, the defense of the nation. 🛡️

NOTES

1. <https://www.merriam-webster.com/dictionary/domain>.
2. DOD Dictionary of Military and Associated Terms, 60, as of March 2017, available at http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.
3. G. Alexander Crowther and Shaheen Ghori. "Detangling the Web – A Screenshot of US Government Cyber Activity". Joint Force Quarterly #78, available at <http://ndupress.ndu.edu/Media/News/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/>.
4. House of Lords. "Protecting Europe against large-scale cyber-attacks". European Union Committee 5th Report of Session 2009–10", page 54, available at <https://publications.parliament.uk/pa/ld200910/ldselect/lddecom/68/68.pdf>
5. The Department of Defense Cyber Strategy, available at https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/.
6. J. Li, Jennifer, and Lindsay Daugherty, "Training Cyber Warriors - What Can Be Learned from Defense Language Training?" Washington, DC: RAND, 2015, http://www.rand.org/pubs/research_reports/RR476.html. See also Spidalieri, Francesca and Jennifer McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies." Arlington, VA: The Potomac Institute, 2016, http://www.potomacinsti-tute.org/images/CDR_Spidalieri-McArdle_pl41-pl63_041216.pdf. Both refer to a 2011 the DOD report "Cyber Operations Personnel Report." Washington DC, 2011, available at <http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf> which report a total of 163,144 military and civilian personnel for FY09: 3777 Defensive Operations, 145,457 Operation and Maintenance and 13,910 Information Assurance. Since this antedates the National Mission Force, we would have to add 6200 personnel for a total of 169,344.
7. U.S. Army. Megacities and the United States Army – Preparing for a Complex and Uncertain Future, June 2014, available at: <https://www.army.mil/e2/c/downloads/351235.pdf>.
8. Joint Publication (JP) 3-0, Operations, January 17, 2017, ix.
9. Statista. "Internet usage in the United States - Statistics & Facts," <https://www.statista.com/topics/2237/internet-usage-in-the-united-states>, accessed August 1, 2017.
10. United States Small Business Administration. "2016 United States Small Business Profile," 2016, https://www.sba.gov/sites/default/files/advocacy/United_States.pdf.
11. Military operations as used here include military or paramilitary operations that other security (such as the Italian Carabinieri) or intelligence forces (such as the CIA) could perform but are mainly military in nature.
12. Technopedia. Information and Communications Technology (ICT). Technopedia goes on to explain that "Converging technologies that exemplify ICT include the merging of audiovisual, telephone and computer networks through a common cabling system. Internet service providers (ISPs) commonly provide internet, phone and television services to homes and businesses through a single optical cable. The elimination of the telephone networks has provided huge economic incentives to implement this convergence, which eliminates many of the costs associated with cabling, signal distribution, user installation, servicing and maintenance costs." Available at <https://www.techopedia.com/definition/24152/information-and-communications-technology-ict>.
13. DOD Directive (DoDD) 5144.02, DoD Chief Information Officer (DoD CIO), November 21, 2014, available at <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514402p.pdf>.
14. DISA. Our Work/DISA 101, available at <http://disa.mil/About/Our-Work>.
15. DISA's Mission Partner Support, available at <http://disa.mil/About/Our-Work/Mission-Partners>.
16. Joint Publication 3-12 (R), Cyberspace Operations, February 5, 2013, II-2, available at http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
17. Geoff Brumfiel, U.S. Navy Brings Back Navigation By The Stars For Officers, National Public Radio, February 22, 2016, available at <http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers>.
18. Major John P. Vickery, The Lost Art of Dismounted Land Navigation. *Infantry Magazine* October-December 2015, available at [http://www.benning.army.mil/infantry/magazine/issues/2015/OCT-DEC/pdf/4\)%20Vickery%20-%20Land%20Nav.pdf](http://www.benning.army.mil/infantry/magazine/issues/2015/OCT-DEC/pdf/4)%20Vickery%20-%20Land%20Nav.pdf).

NOTES

19. Sun Tzu, *The Art of War*, Chapter 13: The Use of Spies.
20. Office of the Director of National Intelligence. Members of the IC. “Eight Department of Defense Elements—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial- Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the four DoD services; the Army, Navy, Marine Corps, and Air Force,” available at <https://www.odni.gov/index.php/what-we-do/members-of-the-ic>.
21. “Lately, a bug that infiltrated the Indian Navy computers at its Eastern Command headquartered at Visakhapatnam enabled Chinese hackers to break into the system. A bulk of sensitive information, which reportedly details the position of marine forces, was compromised in the attack.” Indian Defense. Indian Navy Raises Army For Cyber Front: Recruiting Cadets Against Chinese Hackers, July 13, 2012, available at <http://indiandefence.com/threads/indian-navy-raises-army-for-cyber-front-recruiting-cadets-against-chinese-hackers.20159/>.
22. Washington Post, Hacks of OPM databases compromised 22.1 million people, federal authorities say, available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.9b8cld3e3fcf.
23. G. Alexander Crowther and Shaheen Ghori. “Detangling the Web – A Screenshot of US Government Cyber Activity”. Joint Force Quarterly #78, available at <http://ndupress.ndu.edu/Media/News/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/>.
24. DC3 Web Page, available at <http://www.dc3.mil/>.
25. Justin Ling, Vice.com, “Man Who Sold F-35 Secrets to China Pleads Guilty”, March 24, 2016, available at <https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty>.
26. About the DIB CS Program, available at <https://dibnet.dod.mil/portal/intranet/Splashpage/RegisterThemed>.
27. How Stuff Works, ATM Skimming, available at <http://money.howstuffworks.com/atm-skimming.htm>.
28. Kim Zetter, That Insane, \$81M Bangladesh Bank Heist? Here’s What We Know, *Wired*, May 17, 2016, available at <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>.
29. Mark Pomerleau, Intelligence officials: Cyber domain is still the ‘Wild West’, September 30, 2015, available at <https://defensesystems.com/articles/2015/09/30/ic-congress-cyber-wild-west.aspx>.
30. Examples include the Cyber Intelligence Sharing and Protection Act and the Strengthening State and Local Cyber Crime Fighting Act.
31. This article uses ‘information operations’ to be synonymous with ‘operations in the information environment’, as opposed to the U.S. Army Information Operations specialty.
32. China’s Military Strategy, The State Council Information Office of the People’s Republic of China, Beijing, May 2015.
33. Jeffrey V. Dickey, Thomas B. Everett, Zane M. Galvach, Matthew J. Mesko, Anton V. Soltis, “Russian Political Warfare: Origin, Evolution, and Application”, Naval Postgraduate School, June 2015, available at <https://calhoun.nps.edu/handle/10945/45838>.
34. Stefan Halper. “China, The ‘Three Warfares’”: May 2013, available at <http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf>.
35. Dean Cheng. PLA Views on Informationized Warfare, Information Warfare and Information Operations, 61.
36. Phillip A. Karber, Ph.D. Russia’s New Generation Warfare, NGA Pathfinder, June 4, 2015, <https://medium.com/the-pathfinder/russia-s-new-generation-warfare-471066cb37d#.93qob470m>.
37. Joint Publication 3-0, Operations, January 17, 2017, Chapter III, Joint Functions.
38. Mohammed Jamjoom, ISIS recruiting Western youth with English-language video, CNN, Jun 21, 2014, available at <https://www.youtube.com/watch?v=jdgzCbrPqzQ>.
39. The Carter Center, Religious Appeals in Daesh’s Recruitment Propaganda, September 2016, available at https://www.cartercenter.org/resources/pdfs/peace/conflict_resolution/countering-isis/religious-appeals-in-daesh-recruitment-propaganda-091316.pdf.

NOTES

40. AFCEA, The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict, May 24, 2012, available at <http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf>.
41. RAND, The Lessons of Mumbai, 2009, available at http://www.rand.org/pubs/occasional_papers/OP249.html.
42. Colin Clark. Carter Details Cyber, Intel Strikes Against Daesh At NORTHCOM Ceremony. DefenseOne. May 13, 2016. Available at <http://breakingdefense.com/2016/05/carter-details-cyber-intel-strikes-against-daesh-at-northcom-ceremony/>.
43. Joint Publication 3-05, Special Operations, I-1.

Cyber Threat Characterization

Dr. Kamal T. Jabbour

Dr. Erich Devendorf

ABSTRACT

In this article, we discuss the threat component of the risk to information systems. We review traditional cyber threat models, then present a technical characterization of the cyber threat along ten dimensions. We cross-reference an industry analysis of the Stuxnet threat to illustrate our thinking and conclude with an outline of the threat model application to the development of Cyber Red Books™.

1. INTRODUCTION

In prior work on cyber risk assessment^[1], we referred to the National Institute of Standards (NIST) decomposition of risk into its three constituents of vulnerability, threat, and impact^[2] as the guiding principle for cyber vulnerability assessment. Focusing primarily on developing a repeatable methodology for vulnerability assessment, answering the “what” question of risk, we introduced a characterization of the threat along ten dimensions, from education and training, to resourcing and access.

In this article, we expand our characterization of the threat along these ten dimensions and seek to answer the “how” question of risk. We draw on the analysis of Stuxnet for clarifying distinctions and supporting arguments.

We start the article by reviewing de facto threat models used across the industry and identifying their limitations, and we conclude by outlining the potential application of the threat model to the development of a Cyber Red Book™ to guide security professionals in prioritizing their investments in vulnerability mitigation and mission assurance.

2. TRADITIONAL THREAT MODELS

The cyber risk to an information system is a function of (1) the likelihood of a potential vulnerability, (2) the possibility of a threat exploiting the vulnerability, and (3) the impact of successful exploitation. The potential vulnerability and the impact

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



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

constitute the “what” component of the risk equation, while the threat addresses the “how” question.

A viable cyber threat requires three components:

- ◆ Capability: the talent, time, and treasure to create an adverse impact against a target;
- ◆ Access: remote or physical access to the target system, or access-less, and
- ◆ Intent: which we assume is present.

As we discuss commonly-used models of cyber threat, we caution against the dangers of mirror-imaging—the mistake of attributing to the adversary our way of thinking and our way of fighting. In this historical era of conflict that spans the entire gamut from asymmetric warfare to peer nation-state skirmishes, we cannot afford to dismiss doctrines, cultures or values that differ from ours.

2.1 CYBER THREAT TRENDS

In a 2001 Statement for the Record for the Joint Economic Committee on Cyber Threat Trends and US Network Security^[3], Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, talked about the following potential cyber threats and actors that can challenge the US:

- ◆ National Government threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption.
- ◆ Terrorists are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries.
- ◆ Industrial Spies and Organized Crime Groups pose a medium-level threat to the US through their ability to conduct industrial espionage



Dr. Erich Devendorf is the Director of the Advanced Course in Engineering and Air Force Research Laboratory Early Career Award recipient. As a Computer Engineer at the Air Force Research Laboratory Information Directorate, Dr. Devendorf addresses enduring Air Force challenges at the boundaries between Air, Space and Cyberspace. His assurance work represents a shift away from homogeneous systems to heterogeneous entities designed to complete the mission. He is an internationally recognized creator of multinational, joint training exercises that leverage cross domain fires and multi-domain operations.

and large-scale monetary theft as well as their ability to hire or develop hacker talent.

- ◆ Hacktivists pose a medium-level threat of carrying out an isolated but damaging attack; most international hacktivist groups appear bent on propaganda.
- ◆ Hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures.

Gershwin recognized that globally available tools in 2001 were effective against general-purpose Internet targets, but that specialized tools were needed against hard targets. He also recognized that the skills necessary to develop and employ advanced tools remained a limiting factor for many adversaries.

2.2 GAO THREAT TABLE

In 2005, the Government Accountability Office (GAO) presented a cyber threat table in a report on the role of the Department of Homeland Security in cyber security for critical infrastructure protection^[4]. The threat table included an expanded list of threat actors and their tradecraft:

- ◆ Bot-network operators are hackers who take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks.
- ◆ Criminal groups seek to attack systems for monetary gain, commit identity theft and online fraud. International corporate spies and organized crime also pose a threat to the US through industrial espionage, large-scale monetary theft and their ability to hire/develop hacker talent.

- ◆ Foreign intelligence services use cyber tools in information-gathering and espionage. Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities to enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power.
- ◆ Hackers break into networks for the thrill of the challenge or for bragging rights. While attack tools have become more sophisticated, they have also become easier to use. The large majority of hackers do not have the requisite expertise to threaten critical U.S. networks, but the worldwide population of hackers poses a relatively high threat of an isolated disruption causing serious damage.
- ◆ Disgruntled organization insiders remain a principal source of computer crime. The insider threat also includes outsourcing vendors, as well as, employees who accidentally introduce malware into systems.
- ◆ Phishers execute phishing schemes in an attempt to steal identities or information for monetary gain. May use spam and spyware/malware to accomplish their objectives.
- ◆ Spammers distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations.
- ◆ Spyware/malware authors carry out attacks against users by producing and distributing spyware and malware.
- ◆ Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence.

The GAO table recognizes implicitly the wide range of talent, time, and treasure necessary for each threat category to achieve its objective, with a commensurate range of potential consequences.

3. THE TEN DIMENSIONS OF THE CYBER THREAT

A science and technology examination of recent malicious cyber activity led to the formulation of the following ten-dimensional model to characterize a nation state threat.

3.1 HIGHLY EDUCATED ON THE SCIENCE OF INFORMATION ASSURANCE

Bloom's Taxonomy of Learning^[5] defines six major cognitive categories, ranging from knowledge, comprehension and application, to analysis, synthesis and evaluation. We categorize the lower three cognitive categories under the broad umbrella of training and consider the upper three categories as the foundations of education.

In a 2008 open letter to US universities^[6], Mary Ann Davidson lamented the lack of a secure development lifecycle in the vast majority of degree programs. Davidson called for a revolution in software engineering education, starting with integrating security into the fabric of every course so that engineers can build systems that are safe, secure, and reliable.

In 2011, the White House^[7] added its voice to the chorus calling for scientific rigor in cybersecurity and called for the development of an organized, cohesive scientific foundation that promotes the discovery of laws, hypothesis testing, and capabilities to design and evolve high-assurance systems whose assurance properties can be verified.

While the calls for scientific rigor remain unheeded in US cyber workforce development, evidence points to the opposite in peer nations. Recent results of the annual International Collegiate Programming Contest^[8] reveal the domination by teams from Russia and China, accounting for ten times more top ten teams than US universities. It goes beyond conjecture to conclude that these graduates, highly educated on the science of information assurance, contribute to the cyber capabilities of their nations.

3.2 DOCTRINALLY TRAINED ON THE ART OF CYBER WARFARE

A Preliminary Assessment of National Doctrine and Organization for Cybersecurity and Cyberwarfare^[9] identified 33 states that included cyberwarfare in their military planning and organization. The role of cyber in military doctrine ranged from surveillance and reconnaissance, to information operations against critical targets.

The 1999 thought piece “Unrestricted Warfare”^[10] outlined how two Chinese People’s Liberation (PLA) Army colonels viewed the role of information warfare in compensating for the asymmetrical US advantage in kinetic capabilities. The authors called for unrestricted warfare using all military means against a superior adversary, and provided a doctrinal road map to train Chinese cyber warriors. A 2004 White Paper on National Defense increased the PLA focus on “informationalization” and advocated the use of cyber and electronic warfare in the early stages of a conflict.

In 2010, the Russian Federation discussed the characteristics of modern military conflict in an updated military doctrine that called for the early use of information warfare to achieve military objectives without the use of military force. The 2016 iteration on the Russian doctrine appears defensive in nature, and it focuses on strategic deterrence and prevention of conflicts that might result from information warfare. The Russian doctrine^[11] calls for training cyber warriors by conducting more exercises and practice scenarios of large cyberattacks against multiple targets.

3.3 ADEQUATELY RESOURCED IN TALENT, TIME, AND TREASURE

Contrary to urban legends that portray cyber actors as anti-social teenage prodigies who live in basements and subsist on pizza and soda, the nation state cyber threat enjoys

an abundance of talent, time, and treasure. The mathematical foundations of information theory, signals communications, and encryption necessitate advanced education in these subjects as minimum entry requirements into the field of cyber warfare. The dominant culture of engineering and mathematics in Russia and China, and the large number of universities that deliver the requisite formal education result in a large pool of available talent to fuel cyber warfare.

Besides talent, it takes time to analyze complex missions and systems, map their dependence on cyberspace, and identify potential cyber vulnerabilities. The development of offensive cyber agents that can exploit such vulnerabilities to generate adverse effects requires additional time, and the test and validation of the resulting weapons require even more time. The cycle of mission analysis, cyber dependence, agent development, and test and validation may take several months to a few years.

We estimate treasure in terms of the cost in personnel and materiel resources necessary for the effective generation of cyber effects against a target. We define the cost of personnel in terms of talent and time. Materiel resources include hardware and software computing resources, communication systems for the delivery, and command and control of the cyber agent. Access to a connected target through remote means, or to a stand-alone target by bridging the air gap, also contribute to the necessary treasure.

3.4 THOROUGHLY BRIEFED ON TARGET MISSIONS AND SYSTEMS

Few cyber phenomena have captured the fascination of the media and the general public more than information theft through cyber exploitation and data exfiltration. From the theft of millions of background investigation records from the computers of the Office of Personnel Management^[12] to the widely-publicized theft of US military aircraft trade secrets^[13], a growing body of evidence suggests that near-peer adversaries have acquired detailed knowledge of the design and function of US weapons and systems. Therefore, rather than assume security through obscurity when it comes to hiding the dependence on cyber of critical missions, we must accept as a starting position that nation adversaries are thoroughly briefed on US targets and missions.

Military intelligence points to similarities between foreign and US aircraft as evidence of cyber exploitation of trade secrets from major defense contractors. The recent showcase of the Chinese J-20 stealth fighter revealed numerous similarities to the US F-22 Raptor, leading officials to accuse China of building its aircraft based on stolen designs of the US aircraft.^[14]

Design documentation that permitted an adversary to build a replica of a US weapon may also provide the knowledge necessary to identify and avoid replicating potential cyber vulnerabilities of that weapon. We posit that two possible explanations exist for subtle differences between an original weapon and its replica: (1) a failure to replicate advanced materials and technology, or (2) a deliberate effort to mitigate vulnerabilities in the original weapon.

3.5 MATHEMATICALLY SPECIALIZED IN ARCHITECTURAL PROPERTIES

Architecture encompasses the art and science of design and construction. In cyberspace, architecture refers to the configuration of components and systems that generate, process, store, transmit, consume, and destroy information. Sharing processors, buses, or memory resources creates architectural vulnerabilities that permit the propagation of effects among the processes sharing that resource. For example, an electric short-circuit in one module may trip a circuit-breaker and disconnect other modules, or a system babbling on a bus may prevent other systems from communicating on that bus.

The architectural attribute of resource sharing extends beyond the hardware, software, and networks that compose a system, and includes the users, operators and administrators, as well as, the protocols and policies that govern their roles in the architecture. A formal representation of these relationships provides a mathematical model of potential cyber vulnerabilities and informs threat actors on the ways and means to exploit these vulnerabilities.

A 2010 JASON summer study^[15] concluded that cyber security required an understanding of computer science concepts like model checking, cryptography, type theory, and game theory. These mathematical concepts led to a rigorous framework for examining security, developing a specification, and validating assertions about its correctness under specific assumptions, thereby allowing effective reasoning about program security, obfuscation, and prioritization.

3.6 SUPERIORLY SKILLED IN BYZANTINE FAILURE ANALYSIS

The Byzantine Generals Problem^[16] refers to an encamped army using messengers to communicate among its generals, where one or more generals could be potential traitors. The solution of the problem requires the loyalty of at least two-thirds of the generals to win the battle. In other terms, each traitor can mislead and confuse at most two loyal generals.

Byzantine failure (or fault) analysis in a distributed information system borrows from the Byzantine Generals Problem and reduces the problem of risk assessment to one of vulnerability-consequence assessment regardless of cause. The focus of Byzantine failure analysis turns away from system reliability “when a computer dies”, to system security, “when a computer lies”. In information assurance terms, a Byzantine failure transforms the input vector from compromise in information availability to compromise of information integrity.

A skillful Byzantine failure analysis of a target system provides an adversary with a new attack dimension that seeks to exploit the implicit trust among system components to generate Byzantine behaviors, and consequently adverse effects.

3.7 INTRICATELY INVOLVED IN PROTOCOL SPECIFICATION AND ANALYSIS

Communication protocols serve a valuable function of allowing compatibility and interconnectivity among disparate implementations by different manufacturers. At the foundation of layered communication protocols lies the provision to permit a Layer N+1 implementation to recover from a failure at Layer N. Each protocol layer offers services to the layer above it and receives service from the layer(s) below it. Incorrect specification of protocols^[17] creates potential vulnerabilities independent of specific implementations.

The ubiquitous adoption of commercial protocol standards for military applications brings the benefits of independence from proprietary protocols, compatibility with a broad range of components, and a perception of lower development costs. However, a commercial protocol intended for reliable operation in a permissive environment may exhibit undesirable behaviors in contested operations. In addition, the international organizations that specify, design, and establish protocol standards target their products at common commercial users, without consideration to the risk calculus of military and national security applications.

An undesirable side effect of the globalization of communication protocols may occur as a result of deliberate trade-offs among privacy, reliability, safety, cost, performance, and security. The lack of thorough understanding of the subtle differences among these requirements may result in the hasty adoption of a protocol as a standard without due diligence to mission assurance implications.

3.8 CRITICALLY EMBEDDED IN THE SUPPLY CHAIN

The Department of Defense (DoD) relies on a large number of contractors in the global supply chain, both to build original weapons and to sustain them throughout the decades-long acquisition lifecycle. In a report to Congress, the GAO deemed the DoD supply chain vulnerable to the risk of counterfeit parts, with a potential to disrupt missions and endanger service members.^[18]

While the GAO report did not discuss or infer any malicious manipulation of components through either hardware Trojans or backdoors, the potential adverse mission impact of counterfeit parts is likely independent of intent. As we discussed earlier under Byzantine failures, a bad chip—intentional or accidental—carries the potential of adverse mission effect.

The off-shore outsourcing of electronic manufacturing of integrated circuits and computers brings a unique security challenge at the lowest protocol layer, the physical or hardware layer. Similarly, the off-shore outsourcing of software development of operating systems and tools introduces Byzantine uncertainty at the remaining protocol layers, from the firmware layer all the way to the application layer.

3.9 STRATEGICALLY POSTURED IN COMMAND AND CONTROL

A 2015 GAO Report on Defense Satellite Communications^[19] recognized that the DoD leased commercial SATCOM to support critical mission needs, from command and control of Unmanned Aerial Vehicles (UAV) to intelligence and communications, costing over \$1 billion in 2011. The DoD relies equally on commercial land lines and submarine cables, making a substantial portion of military command and control vulnerable to third-party disruption.

In addition, the GAO quantified further DoD reliance on commercial critical infrastructure in a 2009 report^[20] that referred to the 34 most critical assets whose “incapacitation, exploitation, or destruction could severely affect DOD’s ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions.”

Those critical dependencies on commercial assets render DoD missions vulnerable to threats that could exploit those assets, and expand uncontrollably the scope and range of mission assurance.

3.10 CONVENIENTLY SITUATED FOR ACCESS AND PERSISTENCE

The tyranny of distance characterizes the challenge of fighting a far-off war, even in these days of global connectivity and global mobility. A side effect of fighting abroad is that the adversary enjoys convenient access to resources—spectral, spatial, and temporal. This location convenience translates readily into access and persistence, at times and in places, where the US may find it necessary to establish and re-establish access repeatedly.

4. STUXNET: A COMPLEX THREAT

In this section, we consider Stuxnet in the context of the ten dimensions of the cyber threat, described in Section 3. We chose Stuxnet as an example for three reasons: (1) Experts characterize Stuxnet as the “... first cyber weapon in the world”^[21], (2) Major computer security firms studied, analyzed and reported on Stuxnet and (3) Stuxnet is a sophisticated and targeted weapon. The creator of Stuxnet unequivocally exhibits five of the ten dimensions of the cyber threat. They may possess the other five dimensions, but the data available from Stuxnet does not support that conclusion. Before discussing how the characteristics of Stuxnet map to the capability of its creator, we provide a brief timeline from the initial deployment of Stuxnet until the first speculation of its true purpose.

In June 2009, the first variant of Stuxnet began infecting information systems associated with the Iranian nuclear enrichment program. In January 2010, the International Atomic Energy Agency noticed that Iran was replacing centrifuges at their Natanz nuclear enrichment facility at a very high rate^[22]. Six months later in June 2010, fully patched Windows computers at Natanz began to blue screen and restart. The antivirus software VirusBlokAda identified the cause of these computer problems as a Windows rootkit, first named Rootkit.Tmphider but popularized as W32.Stuxnet^[23]. It was not until 14 July 2010

that Frank Boldewin suggested “... this malware was made for espionage,” on the Wilder Security forum^[24].

4.1 DOCTRINALLY TRAINED ON THE ART OF CYBER WARFARE

The Natanz enrichment facility is a strategically important center of gravity to the Iranian nuclear program^[22]. The International Atomic Energy Agency estimates the nuclear breakout time, defined as the amount of time to manufacture enough high-quality fissile material to produce one nuclear warhead, for a fully functional Natanz facility at 3-6 months^[25]. The critical vulnerability of the facility is the need for contractors to regularly install and replace centrifuges at the site.

Given this vulnerability, the actor that created Stuxnet had a well-scoped and targeted mission that attacked the critical vulnerability for this center of gravity. The Stuxnet payload activates in the presence of specific targets, discussed in Section 4.3 and has natural limitations to stop its spread. Analysis has argued that the creators of Stuxnet took pains to remain compliant with the Laws of Armed Conflict (LOAC)^[26]. The precision and sophistication of Stuxnet coupled with its LOAC compliance demonstrate that its creator was well versed in the art of cyberwarfare.

4.2 ADEQUATELY RESOURCED IN TALENT, TIME, AND TREASURE

The development of Stuxnet extended far beyond the creation of the software used to exploit the target information systems. Before the creation of the core Stuxnet code, engineers had to design a payload to reliably destroy IR-1 centrifuges^[27]. Engineers knowledgeable in machine design and failure analysis designed, developed and tested this payload prior to its employment. Testing requires a significant resource investment to gather the intelligence required to replicate the target system, understand the safeguards in place and construct a representative testbed. With a viable payload, developers created one of the first programmable logic controller rootkits to execute their attack method while simultaneously concealing the attack to avoid detection.

With a viable payload, Symantec estimates the code to deliver that payload to the PLC required a team of five to ten developers working full time for six months^[28]. Other reports suggest that as many as three independent teams worked on Stuxnet to integrate and build its individual modules^[20]. That development included extensive research to evade ten commercial antivirus products and customized memory injection code. In addition to this, Stuxnet utilized four zero day Windows exploits and two certificates stolen from Realtek and JMicron Technology Corps. Collectively, the scope of Stuxnet suggests an actor with adequate resources in time, talent, and treasure.

4.3 THOROUGHLY BRIEFED ON THEIR TARGET MISSIONS AND SYSTEMS

Stuxnet has a well-defined mission set with safeguards in place to minimize and prevent significant spread beyond its intended target. Stuxnet only infects 32-bit systems

in the Windows family from Win 2k through Windows Server 2008 R2. It spreads via USB exploits and over a local area network. These design choices indicate knowledge of both the concept of operations used by its target and the types of systems in use by that target.

Stuxnet uses finer granularity when deploying its payload. The payload only activates when the host system contains the WinCC/Step 7 control software, and it only corrupts the controller when it identifies two specific frequency controllers identified by 7050h and 9500h data blocks^[26]. The actor creating Stuxnet possessed the necessary intelligence to craft and deliver a targeted attack that limits collateral damage while still accomplishing its mission.

4.4 SUPERIORLY SKILLED IN BYZANTINE FAILURE ANALYSIS

Although Stuxnet generated destructive effects against IR-1 centrifuges, security professionals did not discover it until it began to blue screen and reboot Windows systems^[25]. Stuxnet both covered its tracks and generated an effect that was identical to a typical failure mode of a faulty IR-1. The general unreliability of the IR-1 further obfuscated the presence of Stuxnet.

As a Byzantine failure, Stuxnet replicated a failure in the sensors that measure IR-1 performance. This failure resulted in the operator receiving data that made the centrifuge appear to operate normally when it was, in fact, operating outside its design parameters with all safety features removed. The design flaw that enabled this byzantine failure to generate destructive effects is the collocating of the sensor and control feeds for an IR-1.

4.5 CONVENIENTLY SITUATED FOR ACCESS AND PERSISTENCE

Stuxnet's creators deployed it in three distinct waves^[26] starting in 2009 and targeted five distinct contractors that supported the Natanz enrichment facility^[25]. The smallest time elapsed from the Stuxnet compilation to the callback in the first Stuxnet wave was twelve hours^[26]. This short time suggests convenient access to the target. The presence of multiple Stuxnet waves indicates that access to the initial targets persisted for at least a year from June 2009 through April 2010.

The dimensions we identified in our consideration of Stuxnet's creators demonstrate how to evaluate a threat in the context of capability. In addition to these five factors, an argument can be made that its creators were also embedded in the supply chain, had a mathematical understanding of architectural properties and were well versed in protocol specification and analysis. We restricted our analysis to the clearest cut dimensions. In the next section, we discuss the concept of a Cyber Red Book™ that identifies specific capabilities requires to exploit a system.

5. THE CYBER RED BOOK™

In the Spring 2016 issue of *The Cyber Defense Review*, we introduced the Cyber Blue Book™ as a process to codify cyber vulnerability assessment of information systems, to answer in essence the “what” question in cyber risk assessment. We outlined the following ten steps for developing a Cyber Blue Book™:

1. Identify the mission of the System Under Test (SUT).
2. List Mission Essential Functions (MEF).
3. Map cyber dependence of each MEF across the six phases of the information lifecycle.
4. Draw an information boundary for the SUT.
5. Enumerate the Information Exchange Requirements (IER) between the SUT and the outside world.
6. Characterize each information flow across the information boundary.
7. Estimate mission impact of information flow compromise using Byzantine fault analysis.
8. Characterize impact as disruption, degradation, denial, destruction or deception.
9. Categorize vulnerability in terms of architecture, specification or implementation.
10. Design tests to verify the impact of information flow compromise.

The Cyber Red Book™ seeks to characterize the threats necessary to exploit the potential vulnerabilities that the Cyber Blue Book™ identifies. To that effect, Byzantine failure gives way to malicious conduct, and the focus of the inquiry shifts from answering the “what” to the “how”.

In the 2016 paper, we enumerated the information exchanges of a remotely-piloted helicopter, shown in Figure 1, and estimated the adverse effect of a Byzantine corruption to the integrity of the information. Cyber threat characterization requires estimating the threat necessary to compromise the integrity of each information exchange regarding both threat capability and threat access.

For this example, a Cyber Red Book™ examines necessary capability and access:

- ◆ GPS spoofing: signal power, angle and location
- ◆ 3G/4G interference: power and range to jam or hijack
- ◆ Camera and LASER ranging: wavelengths, angle of attack and range

CYBER THREAT CHARACTERIZATION

- ◆ WiFi: based on security protocol, processing power to break encryption and range
- ◆ USB: means to compromise host computer using USB to communicate to the aircraft

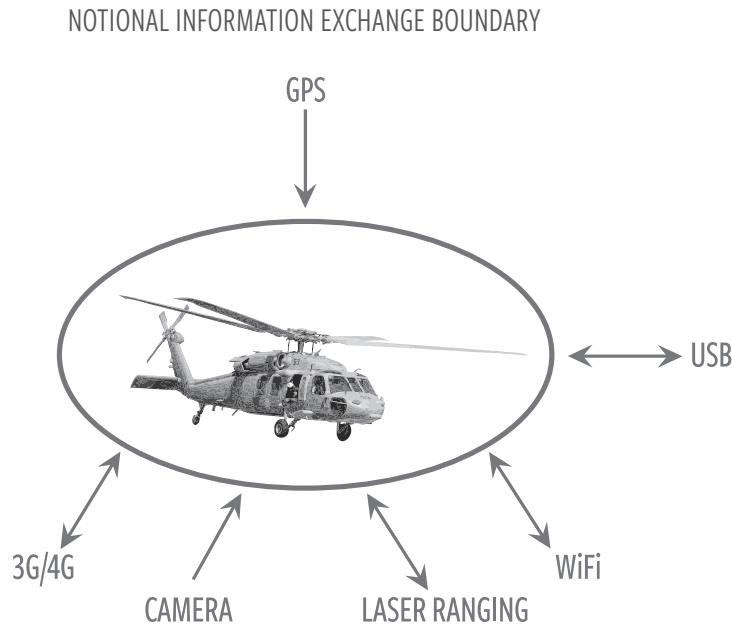



Figure 1. Information Exchange Boundary for RC Helicopter

The Cyber Red Book™ identifies the necessary capabilities to transform a Cyber Blue Book™ failure into a deliberate effect. For the example in Figure 1, at least three dimensions are required to implement a GPS spoof: (1) Conveniently situated for access and persistence, (2) Intricately involved in protocol specification and analysis, and (3) Mathematically specialized in architectural properties.

The nature of the GPS system, low power with line of sight requirements, means an actor must be in close physical proximity to execute a GPS spoof, captured in the first dimension. Effectively spoofing the correct set of GPS packets at the correct power levels to generate an effect requires a strong understanding of the GPS protocol, captured in the second dimension. Finally, an actor must have a strong understanding of the interaction between GPS and the other on-board navigation systems to generate an effect against the platform. That actor requires an even stronger understanding of these interactions to generate the

desired effect. In addition to technology driven constraints, the system concept of operations may require an actor to fulfill additional dimensions to reliably generate their desired effect. The dimensions of a cyber threat provide a set of enduring properties for a Cyber Red Book™ that characterizes risk regarding fundamental actor properties.

6. CONCLUSION

In this article, we discussed the threat component of the risk to information systems. We reviewed traditional cyber threat models, then presented a technical characterization of the cyber threat along ten dimensions. We cross-referenced an industry analysis of the Stuxnet threat to illustrate our thinking and concluded by outlining the application of the threat model to the development of Cyber Red Books™. 

NOTES

1. Kamal Jabbour and Jenny Poisson, "Cyber Risk Assessment in Distributed Information Systems," *The Cyber Defense Review*, Spring 2016, 79-100.
2. Guide for Conducting Risk Assessments: Information Security, National Institute of Standards and Technology, NIST Special Publication 800-30-rev1, September 2012.
3. Lawrence K. Gershwin, Statement for the Record for the Joint Economic Committee on Cyber Threat Trends and US Network Security, June 21, 2001.
4. Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).
5. B.S. Bloom et al, "Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain", New York: David McKay Co Inc., 1956.
6. Mary Ann Davidson, "The Supply Chain Problem", Oracle Chief Security Officer Blog, April 7, 2008.
7. "Trustworthy Cyberspace", Strategic Plan for the Federal Cyber Security Research and Development Program, Executive Office of the President, National Science and Technology Council, December 2011.
8. International Collegiate Programming Contest, Baylor University, 2002-2016.
9. James A. Lewis and Katrina Timlin, Cyber Security and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization", Center for Strategic and International Studies, 2011.
10. Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, February 1999.
11. Information Security Doctrine of the Russian Federation, 2016.
12. Cyber Incidents, Cyber Security Resource Center, Office of Personnel Management, June 2015.
13. Sydney J. Freedburg Jr., "Top Official Admits F-35 Stealth Fighter Secrets Stolen," *Breaking Defense*, June 20, 2013.
14. Alex Lockie, "How China's stealthy new J-20 fighter jet compares to the US's F-22 and F-35," *Business Insider*, November 1, 2016.
15. JASON Summer Study, "The Science of Cyber Security", 2010.
16. Leslie Lamport et al, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, Vol 4, No. 3, July 1982, 382-401.
17. Milica Barjaktarovic, Shiu-Kai Chin and Kamal Jabbour, "Formal Specification and Verification of Communication Protocols Using Automated Tools", First International Conference on Engineering Complex Computer Systems, ICECCS'95, Fort Lauderdale, FL, November 6-10, 1995.
18. United States Government Accountability Office, "COUNTERFEIT PARTS: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," GAO-16-236, February 2016.
19. United States Government Accountability Office, "DEFENSE SATELLITE COMMUNICATIONS: DOD Needs Additional Information to Improve Procurements," GAO-15-459, July 2015.
20. United States Government Accountability Office, "DEFENSE CRITICAL INFRASTRUCTURE: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets," GAO-10-147, October 2009.
21. Sharma, A.R., "Stuxnet-First Cyber Weapon of the World", Symantec, 21 January 2012.
22. Zetter, K., "Countdown to Zero Day", Crown, United States, 2014.
23. T.S., "The Stuxnet Worm a Cyber-missile aimed at Iran?", *The Economist*, September 2010.
24. Boldewin, F., <https://www.wilderssecurity.com/threads/rootkit-tmpbinder.276994/#post-1712134>
25. Heinonen, O., "Iran's Nuclear Breakout Time: A Fact Sheet", POLICYWATCH 2394, The Washington Institute, March 2015.
26. Foltz, A., "Stuxnet, Schmitt Analysis and the Cyber 'Use of Force' Debate", *Joint Force Quarterly*, 67(4), 2012.
27. Langer, R., "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", *The Langer Group*, November 2013.
28. Falliere, N., Murchu, L., Chien, E., "W32.Stuxnet Dossier," Symantec Security Response, February 2011.

Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts

Ralph Martins

ABSTRACT

Warfare in the physical world, both asymmetrical and conventional, has occurred throughout history. However, war in cyberspace is a more recent phenomenon, and there is still much to be explored and understood. Because cyberspace is inherently asymmetric, many lessons learned from asymmetric warfare in the physical world also apply to cyber conflicts. This article will examine the online battle waged by Anonymous against ISIS and analyze five asymmetrical characteristics of cyber conflicts: the vulnerability of conventionally-powerful actors to attacks from relatively weaker adversaries, the unconventional nature of offensive tactics, the low level of intensity of those tactics, the ability of actors to organize and aggressively operate in an extremely decentralized manner, and the strategic goal of breaking willpower or forcing a change of policy. Understanding the asymmetrical nature of cyber conflicts and applying appropriate lessons learned will lead to a more effective defensive posture against cyber-aggressors and facilitate a more secure operating environment in cyberspace.

INTRODUCTION

War in cyberspace is a recent phenomenon, as the first computer networks were implemented only in the mid-20th century. In early 2015, the world for the first time witnessed a public declaration of war by a non-state actor that operates almost exclusively in cyberspace—the collective known as Anonymous—as they openly challenged the Islamic State and their online resources and operations. This conflict has waged on into 2017^[1], and it serves to highlight the many similarities between asymmetrical conflicts in the physical world and conflicts carried out solely online. As a result, many lessons learned from fighting kinetic wars against asymmetrical foes also apply to the fight against non-state actors in cyberspace. This article will examine this battle

© 2017 Ralph Martins



Ralph Martins has over twenty-one years of professional experience as a management consultant and a United States Marine leading teams in the cyber security, cyber warfare and intelligence fields. As a consultant, he has served clients in the Department of Defense and Intelligence Community, and as a Marine, has served in Iraq, Africa, and Cuba, among other locations. He holds graduate degrees in Engineering Management and Military Studies from George Washington University and American Military University respectively and is currently pursuing graduate studies in International Relations at Harvard University. He maintains a number of professional certifications including the Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), and Project Management Professional (PMP).

and analyze the five asymmetrical characteristics of cyber conflicts that make cyberspace an inherently friendly environment for asymmetrical conflicts.

Who Are Anonymous? Why Do They Matter?

Anonymous is a hacktivist collective,^[2] a network of loosely affiliated individuals, groups and other entities with little to no structure, organization or membership requirements that attacks targets in cyberspace and is motivated by various causes often related to freedom of information and human rights. Historically, Anonymous' favorite targets can be categorized as the "big three": big business, big government, and big religious organizations.^[3] Anonymous describes itself as having "a very loose and decentralized command structure that operates on ideas rather than directives."^[4] Major Anonymous operations are typically driven and guided by a very small group of core members relying on their ability to convince other potential supporters of the worthiness of the proposed cause—a process that has historically caused internal friction and disagreement.^[5]

Anonymous' most common online tactics include website defacements, distributed denial-of-service (DDoS) attacks, unauthorized account access, and data exfiltration. To execute DDoS attacks, Anonymous members use publicly available tools such as Gigaloader, JMeter, Low-Orbit Ion Cannon (LOIC), and botnets.^[6] Their tactics are frequently illegal and often cause damage to their targets. As one expert notes,

"...downtime that lasts for hours or days can cost companies thousands in lost revenue or extra bandwidth cost. Participating in a DDoS attack is also illegal, breaking the Computer Fraud and Abuse Act in the United States as well as the 2006 Police

and Justice Act in the United Kingdom; in both countries, perpetrators face a maximum penalty of ten years in prison.”^[7]

While DDoS attacks and the defacement of websites require precious resources (such as time and money) to restore networks, systems, and data to their original state, the more important result is the attention drawn by such attacks. This is where Anonymous makes its most significant impact. The group influences public opinion and government policies by training the proverbial spotlight on its chosen issues through the use of cyberattacks. As an example, Anonymous took on the repressive regime of Tunisian President Zine El Abidine Ben Ali in January of 2011 via the use of DDoS attacks, website defacement, the sharing of cybertools with dissidents, and facilitating the flow of information into and out of the country in support of the rebels.^[8] Shortly after Anonymous initiated its online involvement, Ben Ali dissolved his government and fled to Saudi Arabia. However, around the same time that Ali’s regime was collapsing, the Islamic State was beginning to actively and aggressively oppose the fledgling Iraqi democracy, terrorize Iraqi citizens and spreading its violence to neighboring Syria.

The Rise of ISIS

The Islamic State in Iraq and Syria (ISIS), also known as ISIL, Daesh or simply the Islamic State, is a Sunni militant group attempting to create a worldwide caliphate.^[9] ISIS can trace its beginnings to 1999, when a Jordanian militant named Abu Musab al-Zarqawi, who had previously met and been influenced by Osama bin Laden, formed a group called Jamā’at al-Tawhīd wa-al-Jihād (The Organization of Monotheism and Jihad). In 2004, Zarqawi renamed the group Tanzīm Qā’idat al-Jihād fī Bilād al-Rāfidayn, although it was known as al-Qaeda in Iraq.^[10] The group merged with several other similar organizations over time and went through two significant leadership changes. Zarqawi and several subsequent leaders were killed by US and coalition action, and in 2010, Abu Bakr al-Baghdadi assumed command. Baghdadi leads an organization that, in the opinion of one expert, “has exploited these technologies more successfully than any of its contemporaries in the Islamist world.”^[11]

Throughout its history, ISIS has proven to be especially adept at leveraging cyberspace and, more specifically, social media in order to conduct the full lifecycle of terrorist operations.^[12] Through their online operations, ISIS operatives recruit members, issue operational instructions, disseminate propaganda, and, more directly related to their ultimate goal, provoke fear in an attempt to change the behavior and policy of their targets.^[13] As one defense analyst notes,

Although the overarching message is fear, the Islamic State’s propaganda machine has two distinct functions. In the jihadist organization’s aggressive territorial expansion, its social media postings have served a role once filled by leaflets air-dropped ahead of invading armies, sowing terror, disunion, and defection. Meanwhile, its messaging to the wider global community, however gruesome to many

viewers, serves largely to bind the militants of the Islamic State more tightly together—and rally more sympathetic Westerners to its cause. Both these functions rely almost exclusively on media platforms that were nonexistent a decade ago. ^[14]

ISIS has effectively incorporated online resources into almost every facet of what it does. However, just as cyberspace provides ISIS with a highly effective conduit for operation, it also provides opportunities for opponents to counter these efforts.

What Is Asymmetrical Warfare?

Asymmetrical warfare is a conflict between actors whose military capabilities and power are so unevenly matched that the weaker side must resort to low-intensity, indirect and unconventional tactics and strategies to oppose its stronger opponent(s). However, weaker belligerents in an asymmetrical war do not typically seek the total eradication of their opponents, as is often the goal for conventional belligerents. Instead, the objective of the weaker power—often a revolutionary movement, insurgency, terrorist group or other resistance effort—can range from forcing a change in policy to completely wresting away political power from a government. Recent examples of asymmetrical battles include Al Shabaab's struggle against the Somali government, the Kurdish fight for autonomy against several Middle Eastern nations and the ongoing conflict between Hezbollah and Israel. ISIS's fight against Iraq and Syria is another example of an asymmetrical war.

Upon analysis, it is possible to identify trends and common characteristics of asymmetrical battles in the physical world that differentiate them from conventional wars. Five of the more significant features of these conflicts are: the imbalance of power between belligerents, the reliance of asymmetrical forces on unconventional tactics, the relatively low intensity of these unconventional tactics, the decentralized nature of asymmetrical forces, and the asymmetric force's ultimate goal of breaking its enemies' strategic will-power in order to bring about the change in policy or collapse of an entire government. These elements can be further described as follows:

Imbalance of power: The catalyst for asymmetrical warfare is the clash of two unevenly matched adversaries. The entity with more conventional power—often (but not necessarily) a nation-state—typically maintains a significantly more potent conventional military capability and has access to greater resources and more advanced technology than the weaker force. It is this imbalance of power that compels the weaker force to leverage unconventional tactics to have any chance of opposing the stronger power. Specifically, when an adversary is significantly more powerful to the degree that a conventional battle would be a futile effort, unconventional tactics become necessary.

Unconventional tactics: Unconventional tactics are those that diverge from traditional, standard, direct combat operations. On a traditional battlefield, they include covert action, hit-and-runs, ambushes, subversion, harassment, and the

heavy use of improvised weapons and explosives. This type of combat often requires the ability to blend into an indigenous population so fighters can operate clandestinely and wait for opportune times to strike. Unconventional tactics require fighters to utilize creativity, flexibility, adaptability, extreme mobility, deception, and patience. Unconventional weapons are often cheap, easy to improvise and require less formal training than conventional weapons.

Low intensity: By relying on unconventional tactics, an asymmetrical force, by definition, chooses to forego the use of more conventional and potent tactics, as using these tactics against a conventionally stronger enemy would be unlikely to result in victory. Instead of attempting to precipitate mass casualties and destruction and ultimately land a killing blow, an asymmetrical force aims to wear down the stronger adversary with smaller attacks, often more frequent but lower in intensity.

Decentralization: Asymmetrical forces in the physical world do not have a traditional hierarchical shape in their organizational structures. They are composed of networks of individuals and smaller cells with varying degrees of connectivity to each other. These networks are, by their very nature, resilient and difficult to destroy. And while cells can be eliminated, they can also be easily reconstituted. Each cell is self-sufficient, and destroying the greater organization's leadership does not necessarily render the components (individuals and cells) of that network incapable of operating.

Breaking strategic willpower: Unlike in conventional war, the goal of an asymmetrical force is not the total destruction of its enemy's forces or even the significant degrading of its enemy's ability to fight. Instead, unconventional fighters are often employed as part of a long-term plan to achieve submission, capitulation or retreat by breaking the will of the enemy on a strategic level. It is the willpower of leadership that is the real target of the asymmetrical fighter.

Anonymous and Its Online War on ISIS

Anonymous has been waging an online war against ISIS since 2015—a conflict that demonstrates the asymmetrical nature of cyberspace. This war began with a violent attack in the physical world by a related group. In January 2015, members of Al Qaeda in the Arabian Peninsula (AQAP) carried out several attacks within the city of Paris, highlighted by the shooting at the *Charlie Hebdo* newspaper office.^[15] Anonymous responded to these attacks by launching Operation Charlie Hebdo, promising a “massive” response in retribution and immediately taking down a French extremist website.^[16] Shortly thereafter, Anonymous expanded its attacks to other related militant targets in cyberspace as it initiated Operation ISIS and took down 1,500 ISIS-associated Twitter and Facebook accounts, claiming, “From now on, there [will be] no safe place for you online—you will

be treated like a virus, and we are the cure. We own the internet now.”^[17] Following the November 2015 ISIS attacks in and around Paris that killed 130 people, Anonymous again declared a new war on ISIS and announced Operation Paris to “defend our values and our freedom.”^[18] One member of Anonymous summarized the organization’s perspective on ISIS as follows: “We believe that [sic] all of us combined, we can show the world that ISIS does not have as much power as it claims it does and show the world that if ordinary people can fight ISIS [successfully] then the governments of the world certainly can.” The member continued, “ISIS is a plague on the internet and humanity.”^[19] While Anonymous’ war against ISIS has had its struggles and some members have claimed to have given up the battle,^[20] for many supporters it will continue for the foreseeable future.^[21]

An analysis of Anonymous’ online conflict with ISIS exhibits the five characteristics of traditional asymmetrical forces enumerated earlier. First, Anonymous is taking on an adversary that is clearly stronger regarding conventional power and has access to greater resources. ISIS brought in \$2 billion in 2014^[22] causing it to be labeled the world’s “richest terror group”^[23] and the “best financially endowed terrorist organization in history.”^[24] Anonymous, on the other hand, has no meaningful budget. Instead, it relies on occasional donations^[25] and largely operates by crowdsourcing volunteers of various skill levels to participate in its operations on an ad-hoc basis.^[26] Despite this apparent limitation, Anonymous has demonstrated hacking capabilities to such a degree of sophistication that its ability to confront ISIS online is highly regarded and some experts even consider Anonymous to be a serious challenge to ISIS’s online operations.^[27] This aspect of the conflict, in particular, demonstrates that cyberspace can be “a great equalizer.”^[28]

Second, Anonymous has a highly decentralized presence and leverages the talents of its members from around the world in its online fight against ISIS. The organization has been described as an “online global brain of community users”^[29] and a “decentralized online community of users”^[30] who expend effort “promoting collaborative global hacktivism”^[31] and who are “based around the world and hail from every walk of life.”^[32] However Anonymous might be characterized, it lacks the well-defined organizational structure that would be expected in other groups of similar size. Nowhere is this more evident than in the fight against ISIS. As one think tank researcher describes it:

Like most hacktivist groups, #OpISIS is ostensibly flat and leaderless, though day-to-day operations are sustained by a few dozen long-serving members who form the concrete core of the movement. In turn, they guide the efforts of hundreds of volunteers. Fragmentary groups tend to focus on different things (taking down websites, tagging Twitter accounts, locating propaganda videos, infiltrating jihadi forums), their roles converging and diverging at random. The result is organic and more than a little chaotic. But it works.^[33]

Anonymous leverages cyber-attacks conducted by individuals and teams spread across the globe,^[34] and although collaboration occurs, few, if any, of the participants launching the attacks are physically collocated, and most do not know each other.^[35]

Third, the online tactics, techniques and procedures used by Anonymous against ISIS fit the definition of unconventional. Anonymous has used online mockery,^[36] disruption of communications,^[37] counter-propaganda efforts,^[38] and disruption of finance^[39] to thwart ISIS operations and try “to shut down their ability to talk to the public.”^[40] Furthermore, online attacks are in themselves unconventional in that attack skills are simple and inexpensive to acquire. This is made evident by the fact that hackers-for-hire are relatively cheap^[41] and, despite Anonymous’ lack of an operational budget, some of its most elite members have executed “devastating” attacks on high-profile targets are self-taught.^[42]

Fourth, the online conflict between Anonymous and ISIS is low-intensity, and Anonymous is making use of tactics that are intended to wear down support for ISIS and its effectiveness over time.^[43] Nothing Anonymous has done or can do online (DDoS, website defacements, propaganda dissemination) will likely result in the death of ISIS members or large-scale physical destruction of their resources. This is simply due to the constraints of cyberspace—the inability to create kinetic effects (kill people or break things) via online attacks. All of this means that there will likely not be any powerful or decisive blow, but rather a continuous series of many small, disruptive attacks.

Fifth, because Anonymous knows it cannot destroy ISIS through cyberspace, it instead seeks to contribute to the effort to break its willpower by restricting its operations and eroding its capabilities. Twitter is an effective tool for ISIS propaganda,^[44] and an Anonymous-affiliated group has claimed responsibility for shutting down over 70,000 ISIS Twitter accounts.^[45] In November of 2015, Foreign Policy noted that Anonymous and its cohorts “claim to have dismantled some 149 Islamic State-linked websites and flagged roughly 101,000 Twitter accounts and 5,900 propaganda videos” and then described Anonymous as postured to combat ISIS via the Twitter “town square” and the depths of the deep web.^[46]

The Asymmetrical Nature of Cyberspace

Perhaps similar to Billy Mitchell’s struggle to convince and educate his contemporaries about the potential application of air power in the early 20th century, there is a learning curve to climb in understanding and institutionalizing the knowledge about the operations of cyber actors and the inherent nature of online combat. It stands to reason that as everything from military weapon systems to everyday objects in our lives are increasingly interconnected and reliant on information systems, vulnerabilities and available attack vectors will increase accordingly and therefore so will the frequency and effects of attacks. Anyone who wishes to assert power and influence in the modern, globalized world must recognize and prepare for this obvious trend.

However, cyberspace is more than just a new warfighting domain that will be increasingly conducive to conflict over time. Its makeup is such that it is inherently asymmetrical, as exhibited in the online skirmish between Anonymous and ISIS, and this characteristic is a critical point in understanding the cyberwars of the future. Cyberspace is designed so that actors with relatively little conventional power can impose meaningful effects on significantly more powerful adversaries. Analyst John Arquilla once noted that “The destructive and disruptive power of small groups and even individuals—in the physical world as well as in cyberspace—just keeps growing.”^[47] Scholar P.W. Singer recently noted, “Today, it is the United States that has the conventional edge on its adversaries, and thus many of its attackers see cyberattacks as their asymmetric way to work around a power imbalance.”^[48]

The same highly interconnected architecture of the Internet that allows billions of people around the world to communicate instantaneously also allows for a planet full of potential attackers, making extreme geographic decentralization a standard feature of cyber armies. Hostile actions in cyberspace are also unconventional in nature, as described by retired Army General Wesley Clark: “There is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril.”^[49] But while online attacks are quick, frequent and can be persistent, they are also as yet unable to replicate the kinetic effects of combat in the physical world. With few rare exceptions, such as the tangibly destructive power of Stuxnet,^[50] virtually all conflicts in cyberspace are of low intensity and will, therefore, require a protracted, persistent and committed effort to degrade capabilities and erode willpower over time. By recognizing all these asymmetrical features of cyber warfare, it will become easier to develop strategies to counteract and mitigate threats in cyberspace. 🛡️

NOTES

1. Chris Summers, "Hacker accesses ISIS's radio channel and taunts Abu Bakr al-Baghdadi by saying: 'Mosul will be liberated'", January 13, 2017, <http://www.dailymail.co.uk/news/article-4116338/Hacker-accesses-ISIS-s-radio-channel-taunts-Abu-Bakr-al-Baghdadi-saying-Mosul-liberated.html>.
2. The term hacktivist, a portmanteau of hacker and activist, has been credited by some to the former hacker group Cult of the Dead Cow. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, New York: Oxford University Press, 2014, 77.
3. Quinn Norton, "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down," *Wired*, July 3, 2012, http://www.wired.com/2012/07/ff_anonymous/.
4. ANON OPS: A Press Release, ANONNEWS, December 10, 2010, http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf.
5. Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulSec, Anonymous and the Global Cyber Insurgency*, New York: Little, Brown and Company, 2012, 92 – 99.
6. *ibid.*, 74.
7. *ibid.*, 64.
8. Quinn Norton, "2011: The Year Anonymous Took On Cops, Dictators and Existential Dread," *Wired*, January 11, 2012, <http://www.wired.com/2012/01/anonymous-dicators-existential-dread/>.
9. Matt Bradley, "ISIS Declares New Islamist Caliphate: Militant Group Declares Statehood, Demands Allegiance From Other Organizations," *The Wall Street Journal*, June 29, 2014, <http://www.wsj.com/articles/isis-declares-new-islamist-caliphate-1404065263>.
10. Lawrence Joffe, "Abu Musab al-Zarqawi obituary," *The Guardian*, June 8, 2006, <http://www.theguardian.com/news/2006/jun/09/guardianobituaries.alqaida>.
11. Hisham Melhem, "Keeping Up With the Caliphate: An Islamic State for the Internet Age," *Foreign Affairs*, November/December 2015, <https://www.foreignaffairs.com/reviews/keeping-caliphate>.
12. Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied Media," *New York Times*, August 30, 2014, <http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html>.
13. Faisal Irshaid, "How Isis is spreading its message online," *BBC News*, June 19, 2014, <http://www.bbc.com/news/world-middle-east-27912569>; M.L. Nestel, Gilad Shiloach and Amit Weiss, "ISIS Forums Share Pipe Bomb Instructions for Attacks on NYC, Las Vegas," *Vocativ*, September 16, 2014, <http://www.vocativ.com/world/isis-2/isis-pipe-bomb-attack-america/>; Shiv Malik et al, "Isis in duel with Twitter and YouTube to spread extremist propaganda," *The Guardian*, September 24, 2014, <http://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi>; "Flames of War - AMAZING battle footage," LiveLeak video, 55:14, posted by "KIWalid," September 20, 2014, http://www.liveleak.com/view?i=5c2_1411222393.
14. Emerson Brooking, "The ISIS Propaganda Machine Is Horrifying and Effective. How Does It Work?," *Defense in Depth* (blog), Council on Foreign Relations, August 21, 2014, <http://blogs.cfr.org/davidson/2014/08/21/the-isis-propaganda-machine-is-horrifying-and-effective-how-does-it-work/>.
15. "Charlie Hebdo Attack: Three Days of Terror," *BBC News*, January 14, 2015, <http://www.bbc.com/news/world-europe-30708237>.
16. "Anonymous - #OpCharlieHebdo" YouTube video, 2:58, posted by "Anonymous France," <https://www.youtube.com/watch?v=oqbwqmb8P00>, accessed September 25, 2016; Guest, Untitled, Pastebin, <http://pastebin.com/Pdj2Z0wC>, accessed October 24, 2016; Rose Troup Buchanan, "#OpCharlieHebdo: Anonymous Take Down French Extremist Website After Threatening 'Retribution' for Charlie Hebdo Attacks," *The Independent*, January 12, 2015, <http://www.independent.co.uk/life-style/gadgets-and-tech/opcharliehebdo-anonymous-take-down-french-extremist-website-after-threaten-ing-retribution-for-9972013.html>.

NOTES

17. Wang Wei, "Hacktivist Group Anonymous (#OpISIS) Takes Down Islamic State (ISIS) Social Media Accounts," *The Hacker News*, February 8, 2015, <http://thehackernews.com/2015/02/anonymous-isis-cyber-attack.html>; Rick Gladstone, "Activist Links More Than 26,000 Twitter Accounts to ISIS," *New York Times*, March 31, 2015, http://www.nytimes.com/2015/04/01/world/middleeast/activist-links-more-than-26000-twitter-accounts-to-isis.html?mtrref=undefined&mtrref=www.nytimes.com&_r=0; Andrew Griffin, "Paris Attacks: Anonymous Vows to Avenge Charlie Hebdo Shootings with Cyberattacks on Islamist Websites," *The Independent*, January 9, 2015, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-vows-to-avenge-charlie-hebdo-shootings-with-cyberattacks-on-islamist-9968813.html>; Guest, #OpISIS - Twitter/Facebook, *Pastebin*.
18. Keely Lockhart and Myles Burke, "#OpISIS: Why Anonymous has declared an online war against Isil - in 90 seconds," *The Telegraph*, December 11, 2015, <http://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-Why-Anonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html>.
19. E.T. Brooking, "Anonymous vs. the Islamic State," *Foreign Policy*, November 13, 2015, <http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/>.
20. Russell Brandon, "The Anonymous 'War on ISIS' Is Already Falling Apart," *The Verge*, November 23, 2015, <http://www.theverge.com/2015/11/23/9782330/anonymous-war-on-isis-hacktivism-terrorism>; Jesse Hirsch, "After Orlando, Anonymous Vows To Leave ISIS Alone," *Good*, June 14, 2016, <https://www.good.is/articles/anonymous-says-peace>.
21. Simon Parkin, "Operation Troll ISIS: Inside Anonymous' War to Take Down Daesh," *Wired*, October 6, 2016, <http://www.wired.co.uk/article/anonymous-war-to-undermine-daesh>.
22. Jose Pagliery, "Inside the \$2 Billion ISIS War Machine," *CNN Money*, December 11, 2015, <http://money.cnn.com/2015/12/06/news/isis-funding/>.
23. Jack Moore, "Mosul Seized: Jihadis Loot \$429m from City's Central Bank to Make Isis World's Richest Terror Force," *International Business Times*, June 11, 2014, <http://www.ibtimes.co.uk/mosul-seized-jihadis-loot-429m-citys-central-bank-make-isis-worlds-richest-terror-force-1452190>.
24. Pagliery, "Inside the \$2 billion ISIS war machine."
25. Anthony Cuthbertson, "Operation Isis: Ghostsec Hackers Launch Crowdfunding Campaign in Fight Against Islamic State," *International Business Times*, July 29, 2015, <http://www.ibtimes.co.uk/operation-isis-ghostsec-hackers-launch-crowdfunding-campaign-fight-against-islamic-state-1513104>.
26. Anthony Cuthbertson, "Anonymous #OpParis: Hacktivists Publish 'Noob's Guide' for Fighting Isis Online," *International Business Times*, November 17, 2015, <http://www.ibtimes.co.uk/anonymous-opparis-hacktivists-publish-noobs-guide-fighting-isis-online-1529173>.
27. Ari Levy and Anita Balakrishnan, "What can Anonymous really do to ISIS?," *CNBC*, November 18, 2015, <http://www.cnn.com/2015/11/18/what-can-anonymous-really-do-to-isis.html>; Evan Schuman, "Anonymous Just Might Make All the Difference in Attacking ISIS," *Computerworld*, November 16, 2015, <http://www.computerworld.com/article/3005475/cyberattacks/anonymous-just-might-make-all-the-difference-in-attacking-isis.html>.
28. Mary Louise Kelly, "ISIS Uses Cyber Capabilities To Attack The U.S. Online," *NPR*, April 25, 2016, <http://www.npr.org/2016/04/25/475631277/isis-uses-cyber-capabilities-to-attack-the-u-s-online>.
29. "Anonymous definition," *Technopedia*, <https://www.techopedia.com/definition/27213/anonymous-hacking>, accessed October 24, 2016.
30. Ibid.
31. Ibid.
32. Brooking, "Anonymous vs. the Islamic State."
33. Ibid.
34. Ibid.
35. Rick Gladstone, "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State," *New York Times*, March 25, 2015, <http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html>.

NOTES

36. Jasper Hamill, "Anonymous' Four Weirdest Tactics in ISIS Cyber-War: Here's How Hacktivists Are Undermining the Extremists," *The Mirror*, November 19, 2015, <http://www.mirror.co.uk/news/technology-science/technology/anonymous-four-weirdest-tactics-isis-6859278>.
37. John Shammas, "Anonymous Hacker Reveals How They Will Destroy ISIS and Its Ability to Carry Out Terror Attacks," *The Mirror*, December 1, 2015, <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-6931331>.
38. Chris Smith, "Hackers vs. Terrorists: How Anonymous Wants to Beat ISIS," *BGR*, November 30, 2015, <http://bgr.com/2015/11/30/anonymous-hackers-isis-terrorists-war/>.
39. Hamill, "Anonymous' Four Weirdest Tactics."
40. Callum Borchers, "Operation ISIS: Anonymous Member Discusses How Group Is Waging War on Militant Group," *The Independent*, November 28, 2015, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/operation-isis-anonymous-member-reveals-how-they-are-waging-war-on-the-militant-group-a6752831.html>.
41. Cale Guthrie Weissman, "9 Things You Can Hire a Hacker to Do and How Much It Will (Generally) Cost," *Business Insider*, May 8, 2015, <http://www.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5>.
42. Josh Halliday, "Lulzsec Mastermind Sabu: An Elite Hacker and Star FBI Informant," *The Guardian*, March 6, 2012, <https://www.theguardian.com/technology/2012/mar/06/lulzsec-mastermind-sabu-hacker-fbi-informant>.
43. Hamill, "Anonymous' Four Weirdest Tactics."
44. Brooking, "The ISIS Propaganda Machine Is Horrifying and Effective."
45. CtrlSec, Twitter post, November 13, 2015, 5:10 AM, <https://twitter.com/CtrlSec/status/665109376684961792>.
46. Brooking, "Anonymous vs. the Islamic State."
47. John Arquilla, "Beware the Few," *Foreign Policy*, April 16, 2013, <http://foreignpolicy.com/2013/04/16/beware-the-few/>.
48. P. W. Singer, "How the United States Can Win the Cyberwar of the Future," *Foreign Policy*, December 18, 2015, <http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/>.
49. Wesley K. Clark and Peter L. Levin, "Securing the Information Highway," *Foreign Affairs*, November/December 2009, <https://www.foreignaffairs.com/articles/united-states/2009-11-01/securing-information-highway>.
50. Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *Washington Post*, February 16, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html>; Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, January 8, 2015, <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>; Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," *Time*, March 24, 2016, <http://time.com/4270728/iran-cyber-attack-dam-fbi/>.

Maneuverable Applications: Advancing Distributed Computing

Dr. William Clay Moody

Dr. Amy W. Apon

ABSTRACT

Extending the military principle of maneuver into the war-fighting domain of cyberspace, academic and military researchers have produced many theoretical and strategic works, though few have focused on researching the applications and systems that apply this principle. We present a survey of our research in developing new architectures for the enhancement of parallel and distributed applications. Specifically, we discuss our work in applying the military concept of maneuver in the cyberspace domain by creating a set of applications and systems called “maneuverable applications.” Our research investigates resource provisioning, application optimization, and cybersecurity enhancement through the modification, relocation, addition or removal of computing resources.

We first describe our work to create a system to provision a big data computational resource within academic environments. Secondly, we present a computing testbed built to allow researchers to study network optimizations of data centers. Thirdly, we discuss our Petri Net model of an adaptable system, which increases its cyber security posture in the face of varying levels of threat from malicious actors. Finally, we present evidence that traditional ideas about extending maneuver into cyberspace focus on security only, but computing can benefit from maneuver in multiple manners beyond security.

1. INTRODUCTION

Cyberspace research has focused on applying traditional military doctrine and strategies into this new operational domain^[3]. Two of the more popular concepts and topics have been situational awareness^[4,7] and key terrain^[14]. An essential military principle that has received extensive theoretical investigation is maneuver^[5]. This theoretical research has laid the foundation and created opportunities to build systems that possess the features of maneuver.



LTC William Clay Moody serves as an assistant professor and deputy program director for Information Technology in the Department of Electrical Engineering and Computer Science at the United States Military Academy. A founding member of United States Cyber Command, he served as a Cyber Battle Captain of the Joint Operations Center, cyber defense planner for the Expeditionary Cyber Support Element—Iraq, and cyber capabilities engineer for J33 Current Operations. Clay is a 1998 graduate of Clemson University ROTC with a Bachelor's Degree in Computer Engineering. His graduate degrees are a Master's of Science in Computer Networking from North Carolina State University and a Ph.D. in Computer Science from Clemson.

Maneuver is one of the U.S. Army's nine Principles of War. Maneuver includes the application of combat power to maintain an advantage over the enemy^[15]. The flexible and dynamic employment of resources ensures success by keeping adversarial conditions imbalanced and thus reduces failures, compromises, and vulnerabilities. The non-military use of the word maneuver describes an action that is not random or without purpose, but one that is clever or skillful. In both environments, the word maneuver implies deliberate movement and actions taken to achieve a specific purpose.

Distributed and parallel applications allow the execution of complex computations that previously were deemed impractical. Many recent technological advances have contributed to the widespread growth of distributed computing, namely multi-core processors, multi-processor nodes, high-speed networks, improved storage technologies, and virtualization. Regional and national researchers have combined funding and resources to build expansive, large-scale shared computing clusters to allow more efficient usage of power, space, and cooling to multiple user groups. These shared computing resources have become the standard high-performance computational platforms that annually appear on the list of the most powerful commercially available computer systems. Even with these tremendous achievements, the need for continued progress in resource availability, optimization, and security exists.

Our research is motivated by the increased interest in further defining and abstracting the concept of military maneuver in the cyberspace domain. As such, our research is focused on designing, building, and modeling maneuverable applications. We have coined the phrase “maneuverable applications” to denote the distributed and parallel systems and programs that take advantage of the modification,



Dr. Amy W. Apon is professor and chair of the Computer Science Division in the School of Computing at Clemson University. Apon joined Clemson in 2011 in this position. She was on leave as a rotator at the National Science Foundation during 2015, serving in the Computer and Network Systems Division for several programs, including the Computer Systems Research, Big Data, Smart and Connected Health, and Extensible Parallel Systems programs. Prior to joining Clemson, Apon was the founding Director of the Arkansas High Performance Computing center. She holds an M.A. in Mathematics and an M.S. in Computer Science from the University of Missouri–Columbia, and a Ph.D. in Computer Science from Vanderbilt University.

relocation, addition or removal of computing resources within the application, giving the perception of movement. These resources can be computational, network, or storage, or can be the applications themselves. These actions are deliberate, purposeful and meant to achieve an advantage over adversarial conditions. We have applied this approach to address three important topics within distributed and parallel systems, namely resource provisioning, application optimization, and cybersecurity enhancement.

2. MANEUVER FOR RESOURCE PROVISIONING

The first area of interest for studying maneuver in cyberspace platforms is in the area of resource provisioning. Our work with the Job Uninterrupted Maneuverable MapReduce Platform shows how a big data environment can be provisioned in a university setting within the current investment of high-performance computing. This is achieved by the use of maneuvering of nodes in and out of the cluster.

JUMMP, the Job Uninterrupted Maneuverable MapReduce Platform^[12], is an automated scheduling platform that provides a customized Hadoop system within a batch-scheduled cluster environment. JUMMP enables an interactive pseudo-persistent MapReduce platform within the existing administrative structure of an academic high-performance-computing center by “jumping” between nodes with minimal administrative effort. Jumping is implemented by the synchronization of stopping and starting daemon processes on different nodes in the cluster. Our experimental evaluation shows that JUMMP can be as efficient as a persistent Hadoop cluster on dedicated computing resources, depending on the jump time. Additionally, we show that the cluster remains stable, with good performance, in the presence of jumps that occur as

frequently as the average length of Reduce tasks of the currently executing MapReduce job. JUMMP provides an attractive solution to academic institutions that desire to integrate Hadoop into their current computing environment within their financial, technical, and administrative constraints.

A. Introduction

Hadoop is an open-source software tool used to implement MapReduce^[1], a parallel programming paradigm for computation over large amounts of data using a cluster of commodity computer systems. Many organizations have built large-scale production data centers with dedicated computing resources for Hadoop clusters to support their analytic and scientific computation workloads. Hadoop has rapidly evolved and been adopted, thus creating a complex software ecosystem. System administrators are challenged to provide this service while maintaining a stable production environment. This is especially challenging at a typical centralized research institution where the computing infrastructures are designed to accommodate multiple research applications within existing financial, technical, and administrative considerations.

In an academic research environment, we can differentiate the usage of Hadoop into three different categories. The first category includes research applications that use Hadoop MapReduce as a tool for research purposes. These projects can either use MapReduce programs exclusively or use MapReduce programs as part of a larger workflow in a programming framework. Researchers may spend some time developing MapReduce programs and other necessary components and then focus on executing the programs to achieve the final results. As these are research applications, researchers typically alternate between running the computations and analyzing the produced outputs.

The second category is the study of the Hadoop MapReduce software suite itself. This includes studies of Hadoop MapReduce under different hardware and software configurations, development of improvements to Hadoop MapReduce, and implementations of different alternative parallel frameworks to Hadoop MapReduce. The testing of dynamic execution environments for Hadoop is difficult to do in most existing deployments.

The third category in an academic setting includes users in classroom environments who are attempting to learn to install, operate, and maintain a Hadoop cluster. While these assignments usually have short run times and use small data, the nature of the students' learning curve can lead to unintended consequences. In our experiences, teaching Hadoop MapReduce to undergraduates, we observed repeated problems, such as crashing of the Hadoop core processes, corruption of data on the cluster's storage nodes, and overloading of the cluster as students rush to complete the work before deadlines.

B. System Design

Inspired by military maneuver, our approach is to provision Hadoop as a dynamic execution environment that can be instantiated, utilized, and decommissioned when needed by a user. This is achievable from user space since initialized and starting up a Hadoop cluster does not require any administrative privileges. However, creating individual Hadoop clusters imposes overhead due to configuration, data loading and retrieval, and shutdown of the environment. Permanently dedicating a set of computational nodes to individual users places increased workload on administrators who must set policies for scheduling of Hadoop and non-Hadoop jobs while providing fairness and equal access. Our goal is to facilitate the setup of user-controlled dynamic Hadoop environments that execute within existing scheduling policies, including resource limitation, maximum usage time, and priority preemption, without administrative intervention.

The Hadoop cluster uses a single dedicated node for both the distributed file system metadata server and MapReduce master server. This dedicated node resides outside the control of the scheduler. Each worker node is scheduled as an individually scheduled job, which allows for preemption or failure of the job to only affect a single node of

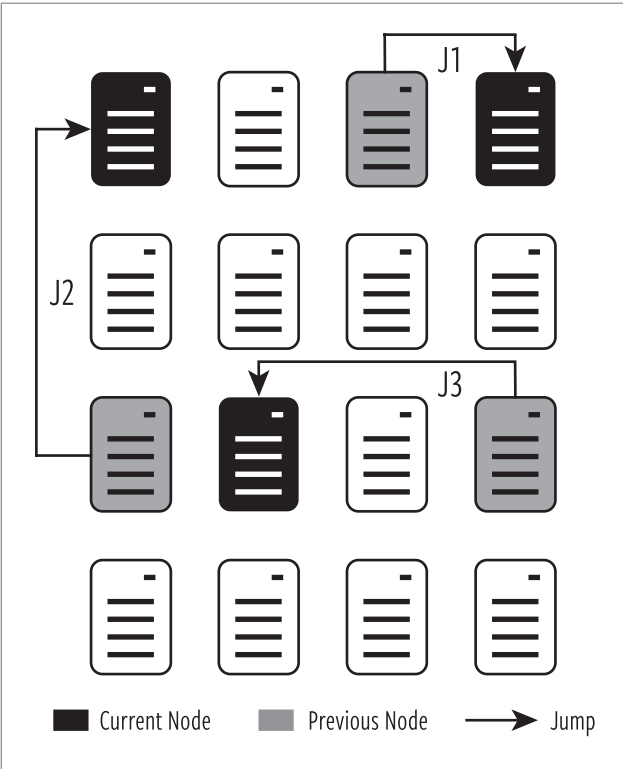


Figure 1. JUMMP maneuvers Hadoop client processing between nodes provisioning a resource within existing HPC environments

the Hadoop cluster. Each data storage and task execution node is established within its scheduled job. The job starts the Hadoop clients and connects them to the persistent head node. Each client waits for its trigger to jump. When the trigger to jump is received, the jumping node schedules its replacement. When notified of an upcoming jump of a slave node, the master node begins to copy the blocks stored on the outgoing node to the remaining nodes in the cluster. The master node immediately kills any task assigned to the outgoing node and reassigns them to available worker nodes. The flexible and maneuverable design of JUMMP allows us to support the user requirements presented above. By allowing

preempted or failed nodes to submit jobs for their replacements, the Hadoop cluster survives, and running jobs continue to execute until completion. Figure 1 illustrates how processes maneuver between nodes in a cluster to perform a big data analysis application.

C. Analysis

Adding maneuverability to a Hadoop cluster will obviously degrade performance. We evaluate this degradation to understand the trade-offs of this system. With each jump of a computational node, additional overhead occurs over a non-jumping cluster. This overhead comes from two separate sources: the scheduler overhead and replication of data blocks. As previously mentioned, JUMMP schedules each client as separately scheduled jobs within the supercomputing environment. Scheduling and queuing delays result in fewer worker nodes being available to perform map and reduce tasks. The JUMMP is undersized when replacement nodes in the queue are waiting to be assigned to an available node. When an existing node leaves the cluster, all blocks that are stored on its local storage must be replicated across the cluster. The master node begins this immediately upon the decommissioning of the outgoing node. This data replication consumes system resources that previously would have been used for the execution of MapReduce jobs.

This degradation is evaluated with two separate experiments on the performance of JUMMP in our HPC environment. The specifications of our system nodes are shown in Table 1. In each experiment, a baseline performance metric is established for a non-jumping Hadoop cluster by repeatedly running the same MapReduce job 100 times over a static dataset. The job is executed three additional times while varying the jump time for the cluster. We record the times of the jumps, the individual task start and stop times, and the overall job run time. With these results, we quantify the overhead of jumping during the execution of a MapReduce job. With the smaller dataset, a node can jump as fast as every seven minutes.

NODE	HP SL250s
CPU	INTEL XEON E5-2665 (2)
CORES	16
MEMORY	64 GB
LOCAL STORAGE CAPACITY	900 GB
NETWORKING	INFINIBAND

Table 1: Individual node specifications inside our compute cluster [12]

The experiments are executed on a homogeneous set of nodes within the local HPC environment to ensure uniformity of test results. All tests are run on an isolated pool of 96 nodes for worker nodes. At the allocation of the initial nodes and creation of the JUMMP, the dataset for the experiment is imported, the nodes start jumping, and the MapReduce job begins to run. We use the dataset and benchmarks from PUMA, Purdue’s MapReduce Benchmark Suite^[11]. PUMA is developed as a benchmark suite to represent a broad range of MapReduce applications exhibiting application characteristics with high/low computation and high/low shuffle volumes. The parameters of the experiments are shown in Table 2.

APPLICATION	WORDCOUNT	TERASORT
DATASET SIZE	50 GB	300 GB
NODE COUNT	8	32
JUMP TIMES [MINS]	7/10/15	20/40/60

Table 2: Experiment Parameters for our evaluations of JUMMP [12]

The experimental results and evaluation show that JUMMP can be as efficient as a persistent Hadoop cluster on dedicated computing resources, depending on the jump time. Additionally, results show that the cluster remains stable, with good performance, in the presence of jumps that occur as frequently as the average length of Reduce tasks of the currently executing MapReduce job. Our work and results show how maneuver can be used to adequately provision a MapReduce resource. Empowered by maneuver, this resource is available within an existing HPC environment with no additional personnel investment. We note that the allocation of resources that do not produce useful work represents a monetary investment. Though we do not quantify this investment, it can be considered a cost of maneuver for resource provisioning.

3. MANEUVER FOR APPLICATION OPTIMIZATION

Our second area of interest for maneuverability in cyberspace systems is application optimization. Our research with the Flow Optimized Route Configuration Engine (FORCE) investigates this enhancement. FORCE is an instrumented, representative network testbed in which the network topology of a cluster can be maneuvered to develop novel approaches to optimize traffic flow and timing of datacenter traffic [6].

FORCE emulates a data center network using a programmable interconnection controlled by a software-defined networking (SDN) controller. SDN combined with distributed and parallel applications have the potential to deliver optimized application performance at runtime. To investigate this enhancement and design future implementation, a data-

center with a programmable topology integrated with application state is needed. The FORCE advances us down the path towards this goal. We also utilize Hadoop as a case study of distributed and parallel applications along with a simulated Hadoop shuffle traffic generator.

The testbed provides initial experimental evidence of support to our hypothesis for future SDN research. Our experiments on the testbed show a difference in application runtime a factor of over 2.5 times on shuffle traffic for Hadoop MapReduce jobs and the potential for significant speedup in warehouse scale data centers.

A. Introduction

Modifying existing production datacenters or creating entirely new experimental ones to investigate the integration of SDN into datacenter networks is costly in time, dollars, and operational output. Historically, researchers have used controlled infrastructure, called testbeds, resembling real systems and networks to experiment on computing advancements. SDN and datacenter researchers can benefit from this approach, providing meaningful discoveries if established with realistic workloads and instrumented to provide constant, measurable results. Our system is an initial step towards providing a capability that leads to developing infrastructure and processes to understand this integration.

Our overall research goal is to investigate the application of maneuver technologies and methods for optimizing the performance and energy efficiency of parallel and distributed applications in a cluster environment. Goals include the study of how the performance of distributed applications is impacted by the network topology of the datacenter^[9]. SDN is a technology that can be used to easily and temporarily reconfigure physical and virtual network topologies. The FORCE testbed is a low-cost experimental platform that uses a networked set of single computers and virtualization to emulate the performance of whole racks of machines in a data center and their applications. The testbed provides an SDN infrastructure that can be used to study how changes in network topology can impact the performance of the applications.

B. Architecture

A novel design aspect of the FORCE is the use of single workstations to emulate an entire datacenter rack that is full of computing nodes. This emulation enables the study of the inter-rack networking traffic for distributed applications at a very low cost, and the study of how topologies impact performance.

The hardware of the FORCE includes one primary server, twelve client workstations, and two SDN-enabled switches. The testbed is extensible and scalable to a very large size. The set of computers used in our testbed is repurposed from upgraded student laboratories and is installed in a location that allows students to have physical access to the equipment throughout the system building and experimentation.

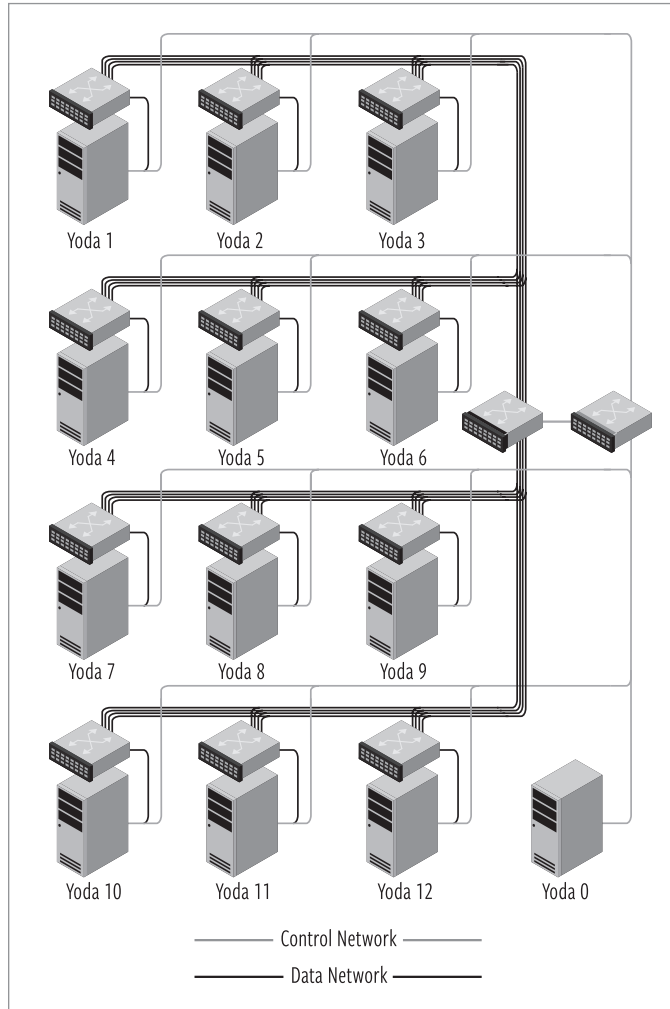


Figure 2. Wire diagram of the Flow Optimized Route Configuration Engine (FORCE) with a maneuverable network topology for application optimization

The two network switches are 48-port gigabit Ethernet switches (Pica8 Pronto 3290 48-port GBe OpenFlow-enabled) using OpenFlow^[10], a popular SDN protocol. Two VLANs are established on one SDN-enabled switch for the “control” and “access” networks. The server and the workstations each have one connection to both of these VLANs. The remaining 48-port switch is connected to one of the four remaining gigabit Ethernet ports of the twelve workstations. This switch allows each workstation to be connected to a maximum of four other workstations with SDN controlled point-to-point connections. This switch is the primary target of the maneuver of the FORCE testbed. Figure 2 provides a wire diagram of the FORCE network testbed.

The core technology empowering the cyber maneuver is a custom virtual topology building package, the FORCE. The FORCE implements a virtual network topology by installing forwarding rules on the SDN switches in a cluster. The topology is described in a series of layers using the NetworkX Python package. Each layer maintains a network graph as well as a procedure for discovering a path between any two vertices. The lowest layer contains information about the physical topology of hosts, switches, interfaces, and links, including characteristics such as hardware addresses and link speeds. The tool then applies subsequent graph layers that abstract each previous layer, building the virtual topology by translating edges into paths on the underlying graph. As a whole, this layered abstraction approach allows mapping of the desired connectivity among vertices on the highest level graph to the lowest level flow rules to be installed onto the SDN switches.

C. Experiment

Hadoop MapReduce is used to demonstrate the utility of the FORCE testbed. The literature^[9] describes the potential speedup of MapReduce shuffle traffic that is possible by maneuvering datacenter racks that contain the Reduce tasks in close network proximity to racks that contain the Map task from the same MapReduce job. This proposed enhancement requires the dynamic reallocation of point-to-point connections between the top-of-rack switches in a two-dimensional torus topology. Our testbed is ideally suited for testing this optimization.

1. Hadoop Shuffle Simulator

The nodes comprising the testbed are not robust enough to run a real workload consisting of multiple Hadoop jobs or multiple virtual Hadoop nodes. To solve this problem, and to ensure that the testbed supports a realistic shuffle traffic network load that corresponds to the traffic between datacenter racks, we implemented a Hadoop shuffle traffic emulator within the FORCE. The emulator executes a centrally controlled software suite that synchronizes bulk network data transfers from Map tasks to Reduce tasks within the cluster. These data transfers are the same as the movement of Map tasks outputs to reducers across the cluster as seen in the shuffle phase of a real MapReduce job.

Given a set of configurations and experiments, the system can deploy the emulated MapReduce jobs across the cluster. These jobs perform the transfer of shuffle traffic. Based on the size of the data to be processed and the system block size, the simulator determines the number of Map tasks required for each job. The number of Reduce tasks is determined by a default global parameter or specific argument on a per job basis. After the system is configured with the number of Map and Reduce tasks per job and the size of the data transfer

between all the Map tasks and the set of Reduce tasks in each job, the transfer of data begins. Since we are interested in studying the inter-rack traffic, any Map and Reduce tasks that reside within the same virtual datacenter rack do not transfer data.

2. Design

The testbed is configured as a 192-node cluster spread over twelve racks. Using bin scheduling as described in^[9] three simultaneous MapReduce jobs are executed running with a single Reduce rack each and three Map racks. There are a total of 1GB of data to transfer from each Map task to its respective Reduce rack. A random placement of datacenter racks is placed into a 4x3 two dimensional torus topology, which simultaneously transfers the simulated shuffle traffic. Each experiment is executed 1000 times. The network topology and the shuffle times needed to complete all the transfers are recorded.

3. Analysis

With this and other experiments, a baseline for comparison with randomized topologies was established by measuring the results with 500 runs using a fixed network topology with no particular distinguishing characteristics. Statistical analysis shows significant difference in the baseline and random samplings. This is our first indication that different topology placements exhibit better and worse congestion characteristics.

Further analysis as shown in Figure 3 shows that worst case transfers times are 2.5 higher than best case transfers. A majority of the experimental runs fall in the middle in a high bell curve. This reinforces our hypothesis that intelligent maneuver of a network topology in a datacenter can maneuver away from worst-case situations, and may be able to maneuver toward optimal situations. These results support further investigation in future work of applying maneuver toward application optimization, specifically network traffic flow optimizations.

Our efforts and results show how maneuver can be used to optimize application performance. Specifically, the FORCE shows how maneuver network topology of the data center can improve the run-time execution shuffle traffic within a Hadoop cluster.

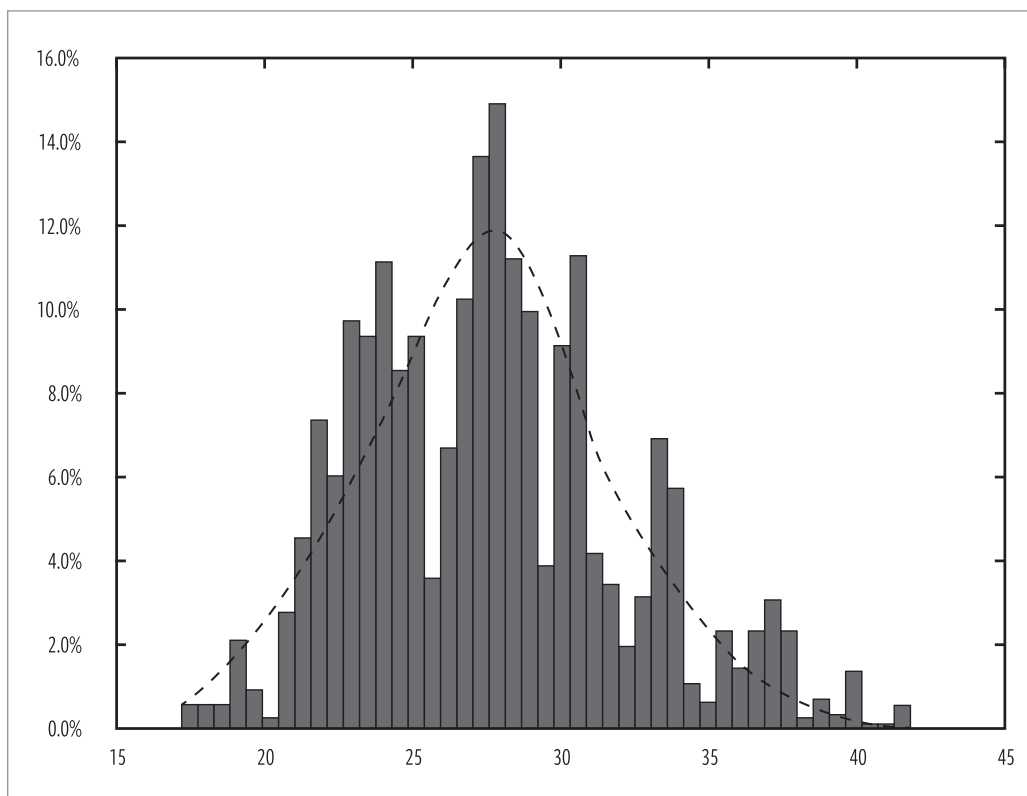


Figure 3. Histogram of simulated shuffle times evaluating the FORCE testbed under random topologies [6]

4. MANEUVER FOR CYBERSECURITY ENHANCEMENT

Our third interest area for studying maneuver in cyberspace is improving cybersecurity. Our work with the Defensive Maneuver Cyber Platform^[8] introduces a Stochastic Petri Net model of improving the survivability of a distributed and parallel application with the additions of moving target defense and deceptive defense, two of the tactics of defensive cyberspace maneuver^[5]. Our extended security analysis of the model provided mathematical evaluations, a prototype simulator of the event, and rules of thumb for employment^[16].

Distributed and parallel applications are critical information technology systems in multiple industries, including academia, military, government, financial, medical, and transportation. These applications present target-rich environments for malicious attackers seeking to disrupt the confidentiality, integrity, and availability of these systems. Applying the military concept of defense cyber maneuver to these systems can provide protection and defense mechanisms that allow survivability and operational continuity. Understand-

ing the tradeoffs between information systems security and operational performance when applying maneuver principles is of interest to administrators, users, and researchers. Our model enables the understanding and evaluation of the costs and benefits of maneuverability in a distributed application environment, specifically focusing on moving target defense and deceptive defense strategies.

A. Introduction

Multiple institutions in academia, industry, and government have discovered the necessity of parallel and distributed computing in data-driven business processes for the solution of complex computational problems. The significant financial investment and operational reliance of these systems create a critical infrastructure that is tightly bound to the success of the organization. The security of these platforms is vital to the survival of these establishments.

Malicious actors seeking financial or intelligence gains are targeting supercomputers and distributed computing centers at an increasing rate. Their methods and efforts to disrupt the confidentiality, integrity, and availability of the systems require network security professionals and researchers to invest remarkable amounts of time and money into protecting these assets.

We are motivated to attempt to improve the security of distributed systems by introducing the military concept of maneuver. Our approach to integrating maneuver into parallel and distributed computing is to add the elements of moving target defense and deceptive defense. The system is designed and modeled using a Stochastic Petri Net in which individual nodes maneuver between three different operating modes. The model is evaluated to understand how the state space and probability distributions are impacted under different configurations.

B. Background

Applegate^[5] introduces four tactics of defensive cyber maneuver. Two of these elements are the subject of this application. Moving target defense is an attempt to change the attack surface of systems to cause an adversary to invest additional resources. This additional expenditure of effort increases the probability of detection, tactic compromise, and failure. Deceptive defense includes presenting decoy and seemingly susceptible systems as attractive targets. These targets are closely monitored and give an early indication of enemy activity while diverting attention away from legitimate and valuable systems. Our research focuses on modeling how moving target and deceptive defense can be integrated into a parallel and distributed computing system.

Petri Nets are a graphical, modeling system for concurrent systems. Visually a Petri Net is bi-partite, weighted, directional graph. There are two types of nodes, a place, indicated by a circle, and a transition, indicated by a straight line or bar. Weighted arcs connect

places to transitions or transition to places. Tokens indicated by dots in the model can be found in places. Places represent conditions of the system while transitions represent actions taken when certain conditions are met. The presence of a token in a place indicates that a certain condition is true. A transition is considered enabled when input places have a number of tokens equal to or greater than the weight of the incoming edges. Enabled transitions can fire in a non-deterministic manner. When a transition fires, it removes tokens from input places equal to incoming edge weights and deposits tokens in out places equal to the weight of outbound edges.

Many extensions to basic Petri Nets exist. One such extension is the Stochastic Petri Net (SPN). Stochastic Petri Nets add a new node called a timed transition, indicated as an unfilled bar. Timed transitions introduce a delay between enabling firings. This delay is a random variable drawn from a Poisson distribution. Each timed transition has its own firing rate for its delay distribution. Once enabled, each timed transition computes its random delay. The timed transition with the shortest delay fires first. SPNs are an extension of Continuous Time Markov Chains and allow their associated mathematical tools to be applied to the analysis of SPNs.

C. System Design

Our system is composed of multiple nodes. Each node can run in one of three modes and nodes are constantly maneuvering between these modes. These modes are operational, idle, or deceptive. An operational node is an active contributor to the computation of the distributed system and is a valuable target that we want to protect. A deceptive node appears to an outside observer to be identical to an operational node by listening to the same network ports and sending and receiving traffic in statistically similar manners. The deceptive node, though, is not doing any constructive work for the system but running a monitoring tool that can detect an intruder, similar to a honeypot^[13]. An idle node is a node that is in neither an operational nor a deceptive state.

In our SPN model, each single node is represented with three places and four transitions. The three places represent the three modes of operation. The four timed transitions are the maneuvers between operational and idle modes and deceptive and operational modes. A node cannot maneuver directly between operational and deceptive modes. Arcs connect places and transitions all with a weight of one. A single token can be found in one of the three places, indicating the current running mode of this node. Timed transitions from operational to idle and idle to operational have the same firing rate. This rate is referred to as the deceptive maneuver rate since that is the rate in which a node maneuvers towards deception. Likewise, the transitions from deceptive to idle, and idle to operation have the same operational maneuver rate.

The entire system is made up of multiple individual nodes with a few configurable parameters. N represents the total number of nodes, O is the minimum number of operational

nodes the system must maintain, while D is the minimum deceptive nodes. It is important that the sum of O and D is less than N so that we can ensure we have a least one idle node so that the system can actually maneuver. The system wide operational maneuver rate is r_o , while r_d is the deceptive maneuver rate. The initial configuration of a system is set to be the minimum values of operational and deceptive nodes. Figure 4 depicts a system consisting of a total of eight nodes with a minimum of three operational nodes and two deceptive nodes.

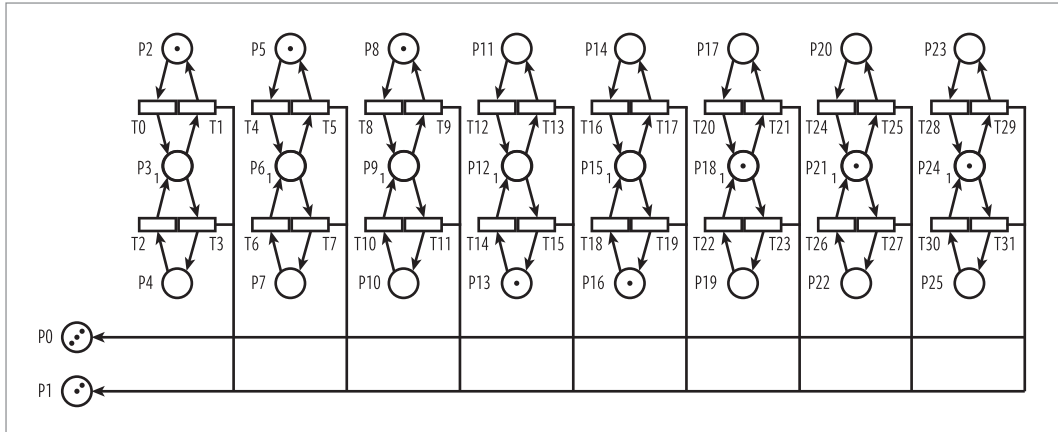


Figure 4. The model of defensive maneuver cyber platform with eight nodes [8]

D. Analysis

To understand all the potential configurations of the system with given set of parameters, we need to quantify the state space of the Defensive Maneuver Cyber Platform (DMCP). As previously mentioned, the system has a defined minimum value for the number of operational and deceptive nodes. Since N is fixed, the maximum value for the count of operational and deceptive nodes can be calculated to be $N-D$ and $N-O$ respectively. The total number of markings or states that the Petri Net can have is quantified by summing the count of valid markings for each valid combination of (o,d) which is the current number of operational and deceptive nodes. This formula is similar to the calculation of computation of multistate combinations since each of the N nodes can be in state operational, deceptive, or idle.

For a given N , the range of possible markings is inversely proportional to the minimum values O and D . The lower the minimum values, the larger the marking state space. The largest state space is when O and D are 0 and is approximately e^N . The minimum value for the state space is when one of the minimum levels of operational or deceptive node is maximized, and the other value is minimized. For instance, for $N = 8$, $O=7$ and $D=0$, there is a minimum of only 17 valid marking. As Figure 4 shows, this minimum plot is approximately on the order of $\log n$.

One of the goals of the DMCP is to allow the system to change the rate of maneuver between deceptive and operational based on the threat conditions. Specifically, alarms and alerts from the embedded honeypots software in a deceptive node along with other external network security information will provide indications when the system should increase the deceptive maneuver rate. During a low threat environment, the operational maneuver rate can be increased so that the system has more operational capacity. We strive to study the impact that the maneuver rate has on the operational and deceptive composition of the system. An open-source SPN analysis tool^[2] is used to calculate the steady state probabilities for the 8-3-2 DMCP shown in Figure 5. The stacked bar chart in Figure 5 presents the probability of states in which there are 3, 4, 5, and 6 operational nodes with varying ratios of the maneuver rates. As Figure 5 shows, as the probability of deceptive states increases, the probability of a deceptively maneuverable cluster rises to more than 95%. As the probability of operational mode increases then the probability of having 5 or more of our nodes operational (thus increasing operational output) rises to more than 95%. These results show that by adjusting the maneuver rates, we can influence the system towards operational or deceptive.

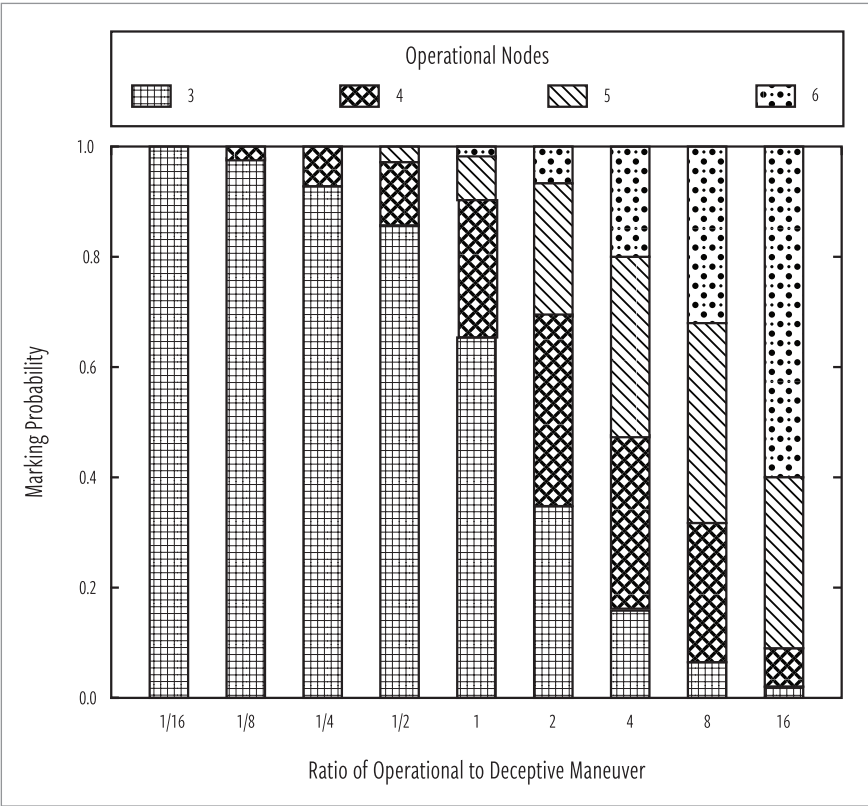


Figure 5. Marking probability of an 8-3-2 defensive maneuver cyber platform when varying the rates of operational and deceptive maneuver [8]

Our attacker model used to evaluate the DMCP is a single adversary who will target only operational or deceptive nodes. The attacker is unable to distinguish between operational and deceptive nodes and selects with equal probability a random active node to target. Once selected, the attacker targets and attempts to gain user or elevated access to the node using its various exploitation tools. After a random amount of time being targeted, the node is considered to be compromised.^[16]

In order to increase the probability of survival, we desire to maximize the probability that a target node is deceptive and the probability that targeted operational nodes maneuver before the node can be fully compromised. We created a series of equations showing how each variable in the system can be adjusted to increase these probabilities. We present a series of rules of thumb for system administrators to employ to find the correct balance between security and operations of a cluster.

Finally, we built a prototype maneuver resource manager to validate the mathematical model. This system incorporates a discrete event simulator allowing each system variable to be adjusted to view the trade-off between operations and security. The system also provides visualization of the current system state, allowing an experimental run to be followed and tracked by researchers. The maneuver manager allows us to refine our rules of thumb for deployment of the system. These models provide the foundation for a system to be built that extends experimentation of the value of cyber maneuver to the security of computing systems.


5. CONCLUSION

We have presented our work in designing, building, and modeling maneuver applications to advance the state of the art in distributed and parallel computing. This work demonstrates how the military concept of maneuver can be applied to distributed computing in multiple facets.

In the area of resource provisioning, the Job Uninterrupted Maneuverable MapReduce Platform deploys a Hadoop cluster within an existing academic high performance-computing (HPC) environment. JUMMP supports high availability and continuous computing for research and education while incurring no additional financial or administrative overhead. It is shown to be as efficient as a persistent Hadoop cluster on dedicated computing resources, depending on the jump time. The cluster remains stable, with good performance, in the presence of jumps that occur as frequently as the average lengths of Reduce tasks.

In the area of application optimization, the Flow Optimized Route Configuration Engine provides the design and prototype development of a datacenter testbed with a reprogrammable network topology. The FORCE testbed includes a Virtual Topology Engine that builds virtual network topologies over physical links with SDN flows and a Flow Network Evaluation system to generate a network congestion estimation score. We highlight the

design and portray the development of a Hadoop shuffle traffic simulator placing realistic loads on datacenter networks. Experimental results indicate placement of computation racks within a datacenter topology potentially has significant impact on the Hadoop shuffle traffic completion time.

Our research into modeling a Defensive Maneuver Cyber Platform with Stochastic Petri Nets demonstrates cybersecurity improvement through maneuver. This model introduces a distributed and parallel application utilizing moving target defense and deceptive defense tactics to increase survivability in the presence of a cyberattack. An SPN model is used to analyze the trade-offs between security and operations in the Defensive Maneuver Cyber Platform. 

ACKNOWLEDGMENT

We would like to recognize the significant contributions of our co-authors on our original works. Jason Anderson, Edward Duffy, Hongxin Hu, Linh Ngo, and K.C. Wang have been extremely supportive and influential in our efforts. Additionally, we would like to acknowledge the hard work of the entire staff of Clemson Computing and Information Technology (CCIT) team in maintaining and administering the Palmetto Cluster and our extensive campus infrastructure. Our work would not be possible without their expertise and effort. This research is supported by part by US NSF MRI Grant #1228312 and US NSF Grant #1405767.

NOTES

1. Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," *Commun. ACM* 51, no. 1 (January 2008): 107–113. doi:10.1145/1327452.1327492.
2. Nicholas J. Dingle, William J. Knottenbelt, and Tamas Suto, "PIPE2: A Tool for the Performance Evaluation of Generalised Stochastic Petri Nets," *SIGMETRICS Perform. Eval. Rev.* 36, no. 4 (March 2009): 34–39. doi:10.1145/1530873.1530881.
3. S. Liles, M. Rogers, J.E. Dietz, and D. Larson, "Applying Traditional Military Principles to Cyber Warfare," In 2012 4th International Conference on Cyber Conflict (CYCON), 1–12, 2012.
4. G. Conti, J. Nelson, and D. Raymond, "Towards a Cyber Common Operating Picture," In 2013 5th International Conference on Cyber Conflict (CyCon), 1–17, 2013.
5. Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," In Cyber Conflict (CYCON), 2012 4th International Conference on, 1–13, IEEE, 2012, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243974.
6. William Clay Moody, Jason Anderson, Kuang-Ching Wang, and Amy Apon "Reconfigurable Network Testbed for Evaluation of Datacenter Topologies," In Proceedings of the Sixth International Workshop on Data Intensive Distributed Computing, 11–20. DIDC '14. New York, NY, USA: ACM, 2014. doi:10.1145/2608020.2608023.
7. J. Dressler, C.L. Bowen, W. Moody, and J. Koepke, "Operational Data Classes for Establishing Situational Awareness in Cyberspace," In Cyber Conflict (CyCon 2014), 2014 6th International Conference On, 175–186, 2014, doi:10.1109/CYCON.2014.6916402.
8. W.C. Moody, Hongxin Hu, and A. Apon, "Defensive Maneuver Cyber Platform Modeling with Stochastic Petri Nets," In 2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaborate-Com), 531–538, 2014.
9. Guohui Wang, T.S. Eugene Ng, and Anees Shaikh, "Programming Your Network at Run-Time for Big Data Applications," In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, 103–108. HotSDN '12, New York, NY, USA: ACM, 2012. doi:10.1145/2342441.2342462.
10. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner, "OpenFlow: Enabling Innovation in Campus Networks," *SIGCOMM Comput. Commun. Rev.* 38, no. 2 (March 2008): 69–74. doi:10.1145/1355734.1355746.
11. Faraz Ahmad, Seyong Lee, Mithuna Thottethodi, and T. N. Vijaykumar, "PUMA: Purdue MapReduce Benchmarks Suite," *ECE Technical Reports*, October 2012, <http://docs.lib.purdue.edu/ecetr/437>.
12. William Clay Moody, Linh Bao Ngo, Edward Duffy, and Amy Apon, "JUMMP: Job Uninterrupted Maneuverable MapReduce Platform," In 2013 IEEE International Conference on Cluster Computing (CLUSTER), 1–8, 2013. doi:10.1109/CLUSTER.2013.6702650.
13. Lance Spitzner, *Honeypots: Tracking Hackers*, Vol. 1. Addison-Wesley Reading, 2003.
14. D. Raymond, G. Conti, T. Cross, and M. Nowatowski, "Key Terrain in Cyberspace: Seeking the High Ground," In Cyber Conflict (CyCon), 2014 6th International Conference, 2014.
15. Department of Defense Dictionary of Military and Associated Terms, November 8, 2010 (last amended July 1, 2017), http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.
16. William Clay Moody, "Designing, Building, and Modeling Maneuverable Applications within Shared Computing Resources" (PhD diss., Clemson University, 2015).

THE CYBER DEFENSE REVIEW

◆ RESEARCH NOTES ◆

Defending the Democratic Open Society in the Cyber Age – Open Data as Democratic Enabler and Attack Vector

Dr. Jan Kallberg

Captain W. Blake Rhoades

Cadet Marcus J. Masello

Dr. Rosemary A. Burk

In the security paradigm, privacy is the major challenge for the security of an open society against cyber threats. In contemporary society, privacy is a lesser security challenge than the threat of an increased attack surface and strengthened attack vectors: Big Data, artificial intelligence, and the massive aggregation of public data. In this research note, we introduce a high-level conflict between interests and societal goals that supersede the privacy and security conflict.

This conflict is between maintaining an open, democratic society with access and dissemination of digital, public information while concomitantly maintaining security. Dissemination of information can create weaknesses primed for cyberattacks by allowing adversaries access to data. Our intention with this research note is to visualize the problem, assess how it can be addressed, and give a direction for future research.

THE DEMOCRATIC OPPORTUNITY WITH OPEN DATA

As a visualization of the democracy-secrecy dichotomy, we turn to Open Data. The voluntary dissemination of public sector information by the government to include Open Data initiatives are intended to strengthen the democracy, lower costs, and increase a societal understanding of the public sector through transparency and accountability. By releasing massive datasets, the government can be studied in detail. Democratic doctrine assumes that, by default, it is beneficial for the constituency to be well-informed, to have access to primary knowledge of the public sector, and that resources entrusted to the public sector are utilized properly. As a democracy, it is pivotal to seek

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



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas under Dr. Bhavani Thuraisingham.

Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

the consent of the governed, and the governed has, by democratic doctrine, to understand governance and the utilization of public resources. The consent of the people is a foundation for the legitimacy and accepted authority of a democratic republic.

President Lincoln stated in a speech in 1854:

I have quoted so much at this time merely to show that, according to our ancient faith, the just powers of governments are derived from the consent of the governed. Now the relation of master and slave is pro tanto a total violation of this principle. The master not only governs the slave without his consent, but he governs him by a set of rules altogether different from those which he prescribes for himself. Allow all the governed an equal voice in the government, and that, and that only, is self-government.^[1]

President Lincoln's speech was not unique; it followed a philosophical tradition from Aristotle, Locke, Jefferson, and forward, who put forth that citizenry of a republic could only succeed if it was engaged and knowledgeable of how society worked. The United States Declaration of Independence says, "That to secure these rights; governments are instituted among men, deriving their just powers from the consent of the governed." Consent from an uninformed constituency is not actual consent and does not contribute to a democratic process, so it has no value as a vehicle for the legitimacy of the republic. The core concept of the democratic republic is that the people will elect representatives based on merit and trust, for the betterment of the people, and that the elected representatives carry out the people's public business as intended by the governed.

Ignorance and lack of knowledge undermine the legitimacy of the democratic republic. Instead of



Captain Blake Rhoades is a member of the Army Cyber Institute's Innovation Team and an Instructor of International Relations in the Department of Social Sciences. From 2012-2013, he was the company commander of the Army's first Cyber National Mission Team at the 780th MI Brigade in Ft. Meade, MD, and has deployed twice as a signals intelligence platoon leader in support of Operation Iraqi Freedom. Blake holds an M.S. in Information Security Policy and Management from Carnegie Mellon University and a B.A. (Political Science) from the University of Alabama. CPT Rhodes recently served as a Madison Policy Forum cybersecurity fellow in New York, NY.

people being governed by fellow members of the republic, they are governed by a faction supported by procedures and empty mechanics. Early on, the Founding Fathers identified the crucial impact of openness for a functional democratic republic, visualized by Thomas Jefferson in his quote, "An informed citizenry is at the heart of a dynamic democracy."

OPEN GOVERNMENT

If we want a professional government and a functional democracy, we cannot surrender the leadership of the republic to bureaucrats. The desire to create an open government with higher accountability, transparency, and efficiency has grown over time and could be seen as a product of our professionalized federal government where the citizenry is the principal, directly or through their elected officials, and the professional public administration is the agent.^[2]

US government initiatives to disseminate digital information accelerated in the 1990s during President Clinton's administration,^[3] continued under President Bush, and received strong support in the early President Obama administration.^{[4][5]} The Federal Office of Management and Budget (OMB) Open Government Directive has outlined a set of principles for Open Data dissemination:

In general, open data will be consistent with the following principles: Public. Consistent with OMB's Open Government Directive, agencies must adopt a presumption in favor of openness to the extent permitted by law and subject to privacy, confidentiality, security, or other valid restrictions.

Accessible. Open Data are made available in convenient, modifiable, and open formats that can be retrieved, downloaded,



Marcus J. Masello is a senior Army ROTC Cadet studying Information Technology at the University of Toledo. At his battalion, he is the Cadet S6 Communications Officer, and on campus participates in the Association of Information Technology Professionals where he is the Director of Membership for its Toledo chapter. Originally from Youngstown, Ohio, he earned his Eagle Scout Award in 2011 and graduated from Boardman High School in 2014. Last summer, Cadet Masello was selected to intern at the Army Cyber Institute at West Point and upon graduation hopes to branch active duty Cyber Corps.

indexed, and searched. Formats should be machine-readable (i.e., data are reasonably structured to allow automated processing). Open Data structures do not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes, often by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.

Described. Open Data are described fully so that consumers of the data have sufficient information to understand their strengths, weaknesses, analytical limitations, security requirements, as well as how to process them. This involves the use of robust, granular metadata (i.e., fields or elements that describe data), thorough documentation of data elements, data dictionaries, and, if applicable, additional descriptions of the purpose of the collection, the population of interest, the characteristics of the sample, and the method of data collection.

Reusable. Open Data are made available under an open license that places no restrictions on their use.

Complete. Open Data is published in primary forms (i.e., as collected at the source), with the finest possible level of granularity that is practicable and permitted by law and other requirements. Derived or aggregated open data should also be published but must reference the primary data.

Timely. Open Data are made available as quickly as necessary to preserve the value



Dr. Rosemary Burk is a Senior Biologist with the U.S. Fish and Wildlife Service, Ecological Services Division in Pacific Northwest Region. She earned a Ph.D. in Biology from the University of North Texas with a specialization in aquatic ecology and environmental science. She has co-authored several articles that have linked failed cyber defense and environmental consequences including *Failed Cyberdefense: The Environmental Consequences of Hostile Acts*, which was published by U.S. Army Military Review in 2014.

of the data. The frequency of release should account for key audiences and downstream needs.

Managed Post-Release. A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements.^[6]

These initiatives have proliferated into state and local government practices including public utilities and other services that are public assets. Further aims of government's online activity are to serve citizens and bring government closer to the people. The Internet empowers people through transparency, e-voting, collecting opinions on public matters, and increasing political self-efficacy among citizens. Since knowledge of the future is unknown, researchers create scenarios for the future state of e-government^[7]; the key question is whether the Open Data increase accountability and transparency. The amount of information the government can publish is immense; however, the publication itself does not automatically translate to trust and confidence from citizens. Open Data can also be a proxy for democracy and bring the government closer to the citizenry. According to its proponents, e-government increases efficiency in service offerings and saves money for the public sector.^[8]

The four ways of disseminating public information described by Suzanne Piotrowski^[9]—public meeting, leaks, voluntarily dissemination and freedom of information request—are driven by other actors than the bureaucracy itself. Piotrowski sees this information sharing as part of the political processes. The voluntary dissemination, which freely accessible Open Data would be, historically has rarely been seen at a global level until recent years. The voluntary dissemination is a political decision. The first countries and states in a federal framework to

actively pursue dissemination enabling citizens' access to Open Data were mainly the US, Canada, UK, Australia, and New Zealand. One reason these countries are more active in dissemination could be the conflict between bureaucratic interest and the interest of the civic societies where Anglo-Saxon countries have a weaker bureaucratic culture in comparison to political structures in centralized governments.^[10]

MAINTAINING LEGITIMACY IN A DIGITAL WORLD

Legitimacy concerns not who can lead but who can govern.^[11] Dwight Waldo believed that we need faith in government for it to have a strong legitimacy; it has to protect, deliver, and promise that life will be better for its citizens. With his long career as a political scientist, Waldo conducted comparisons over several decades. He noted, "a massive amount of evidence indicates a decline in traditional sources and loci for legitimacy."^[12] Waldo raised the question that if the central glue that holds society together is the expectation of more, what does that lead to? Waldo meant that if we build our society around a government that always delivers more services, benefits, and progress, what would happen if there were less of everything in the future? People need a sense that they are represented, and that government is working to improve their lives. In eras of internationalization and globalization, Waldo predicted that government cannot isolate itself from world events.

The idea that internationalization and globalization undermine legitimacy by creating a blurred political landscape is a theme that Robert A. Dahl voices in his book *On Democracy*. Increasing complexity and distance from the population that exists in international organizations, trade agreements, and bilateral agreements play a role in politics and decrease legitimacy; citizens lose the sense that government actions are in the interest of the people. In the "Administrative State," Waldo defined his vision of the "good life" as the best possible condition for the population that can be achieved based on the time, technology, and resources. A legitimate government demonstrates to its citizens that taxes are not collected then squandered and that the return on the taxes makes them worth paying. The government proposes to the population that it can do a better job for all citizens and the charge for those services is taxation. The dissemination of public information becomes instrumental in upholding legitimacy of the government and enables trust in government during difficult times. If the government is no longer considered legitimate, our government and society have failed.

THE ATTACK VECTOR

Open Data releases can appear inconsequential one by one. When taken collectively, the significance of the Open Data can be exploited by adversaries, though the data itself may provide insight into attack vectors. The U.S. Geological Survey (USGS) publishes data regarding water flow, water volume, and measurements from numerous measuring stations throughout a watershed.^[13] National Weather Service (NWS) delivers open data weather information.^[14] The U.S Army Corps of Engineers (USACE) provides detailed information about dams, critical levels, and flow.^[15] The inferences of this data provide insight into

attack vectors. In addition to this open information, the USACE’s detailed database in the National Inventory of Dams (NID) has historically been hacked and compromised.^[16] An adversary can utilize this information to harm the US in a large-scale cyberattack to destabilize the integrity of dams through a watershed.^{[17][18]} This is a single but compelling example, and we have several others that will be a foundation for our future research.


DAMNED IF YOU DO, DAMNED IF YOU DON'T

The US needs transparency to survive as a society and democracy, but how do we do that without creating an unprecedented cyberattack vector into the core of our community? A problem with Open Data is not a single data source by itself, but the aggregated knowledge conceived by mashing data volumes and creating views and understandings beyond the current state.

Then the question arises, how this can be mitigated so the ‘open’ constitutional democracy can maintain its democratic posture and still avoid the creation of a broad attack vector. In the initial study, there are four potential researchable approaches, each of them with their strengths and weaknesses.

APPROACHES TO SOLVING THE DEMOCRACY-SECRECY DICHOTOMY

CONCEPT	SUCCESS-LIMITING FACTORS	INCREASED INSECURITY
Security review before release of Open Data sources.	Requires that you understand the adversarial intent and ability as well as the adversary—which is unlikely.	The security review cannot be one data source at a time, but instead the effect of utilizing several sources. A roadmap for attacks is created in this process.
Strike an equilibrium by assigning metrics for vulnerability and democratic value and run it through a risk model.	First, it is a normative process. Second, the Constitution is not a grayscale where you can pick a place on the scale. You are either constitutional or not.	This model generates less insecurity because it is at a high-level.
Limit security concerns based on a resilience assessment and the rapid responses to patch vulnerabilities in our market economy. The approach is similar to the armoured warfare concept of protection through mobility instead of hardening.	The assumption is that the free market economy is quick to patch vulnerabilities and that any damage can be rapidly contained and mitigated. This would favor the dissemination as a considerable benefit to society than the actual risk. The risk is that the assumption is untested.	The increased insecurity is the risk that the underlying assumption fails. If the assumption fails, then the approach is a passive stance enabling an adversary added target vectors and options.
Open Data is centralized, and all releases are from one major repository, which enables an ongoing risk assessment and ability to limit release if necessary.	Once data is released to the public domain, it cannot be recalled.	The risk is a one-stop-shop for data that the adversary can leverage.

We are early in the learning curve and have not thoroughly researched or addressed the security concerns of Open Data. Initially, the Democracy-Secrecy Dichotomy as it relates to Open Data dissemination needs to be a primary inquiry. How do we strike a balance between living in an Open Society and protecting citizens from the harmful release of data? What can we do to meet both goals? Is there a systematic approach that can be applied? The second wave of inquiry is tailored to address case studies and increase the granularity of the research. 

The views expressed herein are those of the authors and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, the Department of Defense, the United States Fish and Wildlife Service, the Department of the Interior or the United States Government or the University of Toledo.

NOTES

1. Abraham Lincoln, speech at Peoria, Illinois, in Reply to Senator Douglas (October 16, 1854), published in *The Complete Works of Abraham Lincoln* (1894) Vol. 2.
2. Wallace Park, "Open Government Principle: Applying the right to know under the Constitution." *Geo. Wash. L. Rev.* 26 (1957), 1.
3. Patrice McDermott. "Building Open Government," *Government Information Quarterly* 27, no. 4 (2010), 401-413.
4. The White House, "Transparency and Open Government," Memorandum for the Heads of Executive Departments and Agencies (2009), <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2009/m09-12.pdf>.
5. Dennis Linders and Susan Copeland Wilson, "What is Open Government? One Year after the Directive," in *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, ACM, 2011, 262-271.
6. U.S. Government, Project Open Data, Open Data Policy—Managing Information as an Asset, <https://project-open-data.cio.gov/principles/>.
7. Katleen Janssen, "The influence of the PSI directive on open government data: An overview of recent developments," *Government Information Quarterly* 28, no. 4 (2011), 446-456.
8. Jan Kallberg, "The Internet as a Proxy for Democratic Accountability and Transparency---a Comparative Test of Waldo's Five Problem Areas in Five Advanced Democratic Societies," Dissertation, (Richardson: The University of Texas at Dallas, 2011).
9. Suzanne J. Piotrowski, *"Governmental Transparency in the Path of Administrative Reform"*, (New York: SUNY Press, 2007).
10. Paul G. Mahoney, "The Common Law and Economic Growth: Hayek might be Right," *The Journal of Legal Studies* 30, no. 2 (2001), 503-525.
11. David H. Rosenbloom, *"Revisiting Waldo's Administrative State: Constancy and Change in Public Administration"*, (Washington DC: Georgetown University Press, 2006).
12. Dwight Waldo, *The Enterprise of Public Administration: A Summary View*, (Novato, CA: Chandler & Sharp Publishers, 1980).
13. U.S. Geological Survey, Water Watch, <https://waterwatch.usgs.gov/>.
14. National Weather Service <http://www.weather.gov/>.
15. U.S Army Corps of Engineers (USACE) <http://water.usace.army.mil/>.
16. Bill Gertz, "FBI Eyes Chinese Hacking of Dams Database", *Washington Times*, January 6, 2015, <http://www.washington-times.com/news/2015/jan/6/fbi-eyes-chinese-hacking-of-dams-database/>.
17. Rosemary A. Burk, and Jan Kallberg, "Cyber Defense as a part of Hazard Mitigation: Comparing High Hazard Potential Dam Safety Programs in the United States and Sweden," *Journal of Homeland Security and Emergency Management* 13, no. 1 (2016), 77-94.
18. Jan Kallberg, and Rosemary A. Burk, "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," *Military Review* 94, no. 3 (2014), 22.

Multifactor Authentication – A New Chain of Custody Option for Military Logistics

Tom Waters

ABSTRACT

“An Army Marches On Its Stomach,” is a quote attributed to both Napoleon and Frederick the Great.^[1] Both men certainly would attest to the veracity of the sentiment—without secure supply lines, no army can survive for very long. This reliance has grown beyond mere food and now encompasses a broad range of materiel from pencils to remotely piloted drones.

By their very nature, military supply chains are a high-value target for thieves, saboteurs, and counterfeiters. Fraudulent materials, particularly those switched out for high-grade defense aerospace technologies, represent a serious risk to military operations. When materials that can't meet military standards fail in combat situations, it is the warfighter or the innocent bystander who pays the price.

Two-factor authentication has emerged as a reliable metric for mobile device security. What began with only a small smattering of authentication dimensions is now morphing into a range of options that, properly considered, will provide logistics personnel with the necessary assurances their authentic cargo is delivered safely.

Military freight must often pass through multiple civilian supply chain way points, from maritime freight to industrial warehousing, to 'last mile' delivery at forward operating bases by contractor personnel. This creates numerous opportunities for shipment interception, tampering, and replacement.

Counterfeit materials, particularly of aerospace and communication components, represent a significant threat to military operations when these fraudulent supplies don't meet military specifications.



Tom Waters leads a small intelligence team for a Fortune 200 corporation, crawling behind Silicon Valley's headlines to research the global tech market—mobile devices, autonomous vehicles, social media, data analysis, streaming technologies, and e-commerce. He previously served undercover for the Central Intelligence Agency, helping protect U.S. technologies and intellectual property from theft by foreign agents.

Tom has been a guest lecturer at the Naval Post Graduate School, the University of South Florida, and Johns Hopkins University. He is also a popular speaker at technology conferences in Silicon Valley, New York, and the UK. He holds several patents on digital authentication technologies and is the co-inventor of Transactional Key-Pair Encryption, a new Public Key protocol for the quantum computing age.

BACKGROUND

Two-factor authentication has reduced incidences of fraud, including identity theft, in e-commerce. Consumers are no longer at high risk from thieves due to the compromise at a single point of failure in a transaction. Two factors—for a Personal Identifier Number (PIN) and an RSA token—are force multipliers, dramatically improving the security of online transactions.

An explosion of mobile phone applications, or apps, are taking advantage of these technologies. And in doing so, we're seeing innovative new options for increasing the force-multiplication of multifactor authentication. Supply chain and logistics software can leverage these technologies. The potential for protecting military supplies from theft or counterfeiting is in its infancy, but the potential savings, in time and treasure, are considerable.

JUST IN TIME DELIVERY

For years, online retailers like Amazon have had robust, networked systems in place for orders, shipping, and delivery. What began with the simple delivery of books has expanded into an array of skillfully delivered expensive electronics, fashion items, and even wine. These brands are highly coveted, exclusive, and expensive—making them ripe targets for counterfeiters and thieves.

Amazon and its myriad of copycat imitators have changed the logistics industry in ways no one could have imagined. These increasingly predictive systems have in turn spurred new research into the art of the possible for supply chain vendors. With the coming advent of smart-packaging, materials can know where they are and what conditions they've experienced along the way. Supply chain-of-custody software applications can be designed to provide complete end-to-end authentication, ensuring that what is delivered is the actual item that was ordered.

Two-factor authentication originally formed around three basic credentialing criteria; *something you know*, *something you have*, and *someone you are*. These are relatively straightforward to implement at the desktop PC level.

- ♦ *Something you know* – a PIN or Password created by you
- ♦ *Something you have* – an RSA token or other hardware keyfob assigned by an authority
- ♦ *Someone you are* – a biometric sensor registered as you

Two-factor authentication has existed for secure communications systems for years. But moving the process to a mobile environment provided some unique challenges before specific solutions were introduced.

Tokens and USB-based key fobs for PC access are fine—but people do not want to have to carry them around to use with a mobile phone. There are few plug in ports for USB's, and RSA tokens are inconvenient when one hand is already dedicated to holding the smartphone. Taking both outside, away from office environments, provides lots of opportunities for loss, driving up costs and increasing delays in accessing systems. Fortunately, innovation followed mobility.

Each mobile phone has a number assigned to it—several numbers in fact. There is the phone number someone calls to reach the phone's owner. That requires a government identification and some method of payment, generally, a credit card billed to that person.

There is the SIM card the carrier uses to identify the phone owner's account. SIM cards can be swapped between devices to use a single data subscription plan on multiple devices. They carry a small amount of data on board, with varying degrees of security, and some can store credentials for credit card purchases.^[2]

There is also the IMEI, the International Mobile Equipment Identity number, a fifteen-digit number used by cellular networks to identify specific devices on the network. But the IMEI is only utilized for the smartphone device, the hardware. It provides no insight into the user and whether or not they have the authorization to use the device.

So on the surface, one might think that these three numbers would be adequate to authenticate a user. But between the cloning of a cell phone number, the hot-swapping of SIM cards between devices, and the singularity of hardware-specific IMEI the basic ease of stealing the information remains. There's an old saying in cybersecurity—amateurs try to break the encryption, while professionals just steal the keys. The phone number, SIM card, and IMEI are those keys, and all are reasonably easy to steal in one way or another.

This is why fingerprint sensors came into general use. There is a common misconception that the sensor takes a photograph of the fingerprint image and stores it on the device for

comparison when a new fingerprint is presented for comparison. But this is incorrect—the accompanying software turns a fingerprint’s pattern of whirls and loops into a mathematical algorithm. When authentication is requested, it compares the mathematical score of the newly presented fingerprint to the one stored on file. If there is a statistically significant match, the phone is unlocked.

Fingerprint scanners are reliable and have brought new security to mobile devices. Apple based the 2011 debut of their Apple Pay online service to the fingerprint scanner, and Android devices quickly followed with their sensors. Fingerprint authentication is now widely accepted for payments from vending machines to Uber rides across town. It improved trust and reliability in mobile devices as financial tools. This, in turn, has spawned an industry of developing applications that can leverage and expand this trust model.

NEW MODELS OF AUTHENTICATION

The field of potential authentication technologies that are available on smartphones and other devices commonly used by military and civilian personnel are exploding, with new types and dimensions coming online regularly. Among these are:

Location Proof

Using the GPS chips in modern smartphones, logistics planners can simply and securely know when a package has passed from one part of the supply chain into another. This could be a pallet offloaded at a port, or a single package being dropped off via courier. In either case, capturing the GPS coordinates from a consumer device creates yet another layer of security in a chain of custody.

Possession Proof

Radio Frequency Identification (RFID) technologies have been around for years, and are common in industrial and warehouse settings for on-location use. Smartphone technologies have now improved to where systems can incorporate RFID chips on shipped materials. Smartphone cameras can take pictures of Quick Read, or QR codes frequently used by national shipping companies like UPS or FedEx. These commercial applications have significantly reduced the costs of the associated hardware and software, spinning off a litany of third-generation software applications useful to the military.

Access Proof

Many consumer smartphones have data plans with very high fees. For this reason, users are often highly selective of which smartphone applications they allow to access a cellular-based data plans. For these users, local Wi-Fi is a cost-effective option for by passing expensive cellular plans. Corporate providers of shipping and logistics services can use this technology as another dynamic

layer of security. Allowing someone onto their Wi-Fi, or company IP address provides another proof-of-authority in a multifactor environment.

Proximity Proof

QR Codes and RFID are fine for pallet and package authentication. But what if supply chain officers want to confirm proximity to other military hardware? Pilotless drones, autonomous vehicles, or delivery robots can utilize short-distance communications technologies like Bluetooth or ZigBee to authenticate a close (3-5 feet) exchange of materials that can easily be captured and archived.

Behavioral Proof

Behavioral biometrics is the latest iteration of authentication technologies, and likely will be one of the hardest for bad actors to crack. The way each of us signs our name is unique. Though a bad actor could trace a legitimate signature over a capacitive-touch screen tablet, all it could do is reproduce the final image.

The speed of motion, change of direction, curvature of the letters, and even the pressure applied with a stylus pen is unique to each person. Like a fingerprint sensor, signature authentication stores a unique mathematical algorithm. The behavioral requirement to reproduce it creates a unique, on-demand authentication dynamic that has a high degree of reliability.

Confirmation Proof

Sending a one-time text to a cell phone number associated text message system or email address is an increasingly common authentication vector. These one-time codes are easily archived and associate with the individual tied to that number and (messaging or email) service. Many U.S. banks have adopted this for confirming mobile-device access to financial accounts and services.

Witnessed Proof

Among their other similarities, a common denominator between drones and smartphones is the ubiquitous use of cameras. Smartphone camera quality has been rapidly increasing over the past few years, and even low-cost units can now rival some SLR cameras for picture quality.

From sporting events to criminals caught in the act live, consumers are recording moving images and broadcasting them worldwide. This same technology can also be used as a type of video-centric Notary Public, where the handoff of a particular cargo can be captured from the air or surface and archived permanently.

Radio Proof

A new technology that is ‘available’ but disabled on most smartphones is an FM radio chip. Several unique dual or multi-channel authentication strategies are

possible if carriers and manufacturers chose to activate this component. Fortunately, once that decision is made, a simple over the air software upgrade will enable the chip to work again. (The same process Tesla uses to upgrade the software on their cars.)^[3]

These different modalities, taken together, provide a unique and dynamic authentication environment for DoD supply lines. Authentication doesn't have to follow a standard (read: predictable) playbook. It can adjust on the fly, requesting different proofs based on environment, timing, classification, risk, and operational complexity.

What's more, the database-friendly nature of these technologies opens an array of modeling options. While a 'central' database structure is preferable under a typical commercial model, military planners can use distributed databases that are linked together for data sharing purposes. In doing so, not only is the data automatically backed up, but it can also be mined for a variety of fraud detection purposes.

Statistical regression and other analytical techniques can be performed in near real time looking for commonalities where cost saving measures can be applied. They can also search for outliers, evidence of anomalies that need to be investigated while the potential perpetrators are still in theater. These could identify insider threats (theft), external actors (counterfeiters), and organized hackers (state or non-state criminal elements).

This 'Supply Chain of Custody' superficially resembles a block chain, but it's nothing of the sort. Block chain is a distributed authorization system, whereas this is a distributed participation system—one built around a centralized DoD authority (i.e., the military maintains control). Military elements could share information across services, from regular forces to SOF elements, and from full-time service personnel to Reserve units quickly and securely. It also assists in the final disposition of military items—either disposed of in theater, returned via military channels, or shipped through contracted commercial vendors. A chain of custody remains in place for the materials from cradle to grave, eliminating military surplus from falling into the wrong hands.

CONCLUSION

Military leaders will not need to be convinced to 'try' these options; they will welcome the opportunity to add authentication, authority, and auditing tools to their supply chain. The cost of application development is not quite commodity-level yet, but it is getting closer every day. The ability to share information from forward elements, to rear echelon, to HQ elements, to commercial suppliers has never been easier, more cost effective, or secure.

Military personnel frequently use ride sharing applications like Uber to get from one place to another. Platform software applications like this provide bona fides within the system itself, protecting both the driver and the passenger. They are simple, well designed, secure, and accepted by members of the civilian and military population.

There is no reason logistics planners can't use similar software platforms to increase their efficiency, reduce waste, and prevent fraud from interrupting supply lines using the same technology. Multifactor authentication is the future of logistics, and military planners can be among the first to benefit. 🛡️

NOTES

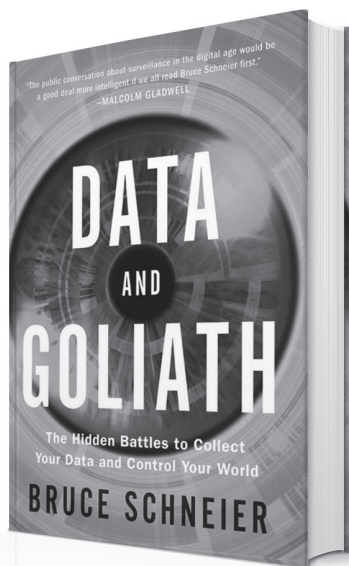
1. Defense Procurement International 2011; Camp and Base Solutions; “An Army Marches On Its Stomach”, accessed April 30 2017 from http://www.electrothermal.com/adminimages/Electrothermal_editorial.pdf.
2. Daniel Bader, “What is a SIM Card and What Does It Do” iMore (Online Magazine), accessed on April 30, 2017 from <http://www.imore.com/what-is-sim-card>.
3. Alex Brisbourne, “Tesla’s Over-the-Air Fix: Best Example Yet of the Internet of Things” Wired Magazine February 2014, accessed April 30, 2017 from <https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things>.

THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆

Data and Goliath:
The Hidden Battles to
Collect Your Data and
Control Your World
by Bruce Schneier

Reviewed by Dr. Jan Kallberg
and CDT Monte Ho



We all surrender privacy in some form and fashion and allow companies to gather data so these enterprises can better serve us. Our cell phone provider needs to know where we are to route calls to the appropriate cell tower. As consumers and users, we allow the cell phone company to track and follow our moves because the convenience of being able to receive a call is greater than our perceived loss of privacy. For the last twenty years, Americans have accepted that the benefit of convenience outweighs the loss of privacy. Bruce Schneier makes a strong argument that this construct should no longer be the case. The book *Data and Goliath* has a compelling message that is a Red Thread of a question through the text: “Do you accept the surrender of your data for convenience?” The author is an authority in the field of cybersecurity—a renowned computer scientist and cryptographer. Schneier has been at the forefront of cybersecurity developments since the 1990s with an appetite to address current challenges and put them in perspective.

Schneier has divided the book into three parts: “Part One: The World We’re Creating,” “Part Two: What’s At Stake,” and “Part Three: What To Do About It.” The author marches forward in the first two sections and slows down in the last part where he gives policy advice to corporations and governments. In Part Three, Schneier sets a foundation by explaining the value of basic societal principles as transparency, accountability, oversight, security versus privacy, and creates a value statement about a decent society. According to Schneier, society has more to gain from increased transparency than

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



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

secrecy, and when secrecy is needed an anchored oversight relying on our democratic values is crucial for a proper balance. Just because the data is there, or accessible, for the government to use it does not warrant its usage without a proper assessment of the need and justification. The author provides numerous examples, which visualize the problem; US Cellular in 2012 received two judicially approved wiretaps and 10,801 subpoenas for identical information without legal review or judicial oversight.

Schneier's examples of ethically over-stretching usage of data, or access to data, point to a critical need for structured norms of accepted and non-accepted behavior. The author points out how this improved behavior can align to the corporate interest and traditional business values and still support the core interests of the government. Schneier shares his vision—and drives home this penetrating argument.

The author provides numerous examples of how the collection of data occurs and explains the utilization of massive data repositories. Schneier describes how the sense of being anonymous by not providing personal information is spurious when inferences from different data sources can provide detailed information and understanding.

Even if readers do not agree with Bruce Schneier, and we are all entitled to our own opinion, there is a significant benefit embedded in this work with the straightforward explanations of what different services do with our personal data. The 120 pages of notes with comments, sources, reflections, and the granular information is an absolute encyclopedia of electronic surveillance, concerns, and real-life events that have occurred in our society. As a reader, diving into the references and following them from source to source is a book by itself in discovery and understanding.



Cadet Monte Ho studies Computer Science at West Point. She is also the cadet executive officer of the Army West Point Cycling team, which is nationally ranked first by USA Cycling in Division II for 2016-2017. She is originally from Los Angeles, California and has participated in two Computer Science AIADs, one through the USC Institute for Creative Technologies in Playa Vista and another at Picatinny Arsenal involving SCADA/ICS. Upon graduation, she hopes to branch Cyber, Signal Corps, or Military Intelligence.

Bruce Schneier has in *Data and Goliath* brought complex issues like security versus privacy, the mechanics behind Big Data, the “hidden” surveillance is massive data generated on a daily basis and the loss of control over your information to light. The book is a significant contribution to the field that is well worth reading. 🛡️

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World

Author: Bruce Schneier

Publisher: W. W. Norton & Company; 1ST Edition
(March 2, 2015)

Hardcover: 400 pages

Language: English

ISBN-10: 0393244814

ISBN-13: 978-0393244816

Price: \$15.00 Hardback

\$10.00 Kindle Edition



13TH International Conference on Cyber Warfare and Cybersecurity

National Defense University
Washington DC

MARCH 8-9 2018

TOPICS FOR ICCWS 2018 WILL INCLUDE:

- ◆ Cyber Warfare
- ◆ Cyber Defence
- ◆ Cyber Terrorism
- ◆ Cyber Security
- ◆ Cyber Crime
- ◆ Cloud Security
- ◆ Social Networking
Threats
- ◆ Big Data Security
- ◆ Psychological
Warfare
- ◆ Digital Forensics

AND MORE ...

Now in its 13th year, the *International Conference on Cyber Warfare and Cyber Security* (ICCWS 2018) is an established platform for academics, practitioners and consultants from around the world involved in Cyber Warfare and Security research to come together and exchange ideas. There are several strong strands of research developing in the cyber warfare and cyber security area including the understanding of threats and risks to information systems, the development of a strong security culture, as well as incident detection and post incident investigation. New threats brought about by social networking and cloud computing are gaining interest from the research community, and the conference is tackling these issues.



The conference is being hosted this year by the National Defense University (NDU) in Washington DC. NDU is an internationally recognized graduate-level university with five colleges and multiple centers of excellence focused on joint education, leader development, and scholarship in national security matters. ICCWS is an excellent opportunity to meet researchers in the fields of cyber warfare and cyber security from around the world. The conference typically has representatives from more than 20 countries and much collaborative work has been initiated from connections made at the conference. The conference proceedings is a book published with an ISSN and ISBN and is indexed by numerous organizations, including Thompson WOS and Elsevier Scopus. Researchers publishing in the conference proceedings also have the opportunity to develop their research for publication in well-renowned journals who partner with the conference.

13TH International Conference on Cyber Warfare and Cybersecurity

National Defense University
Washington DC

MARCH 8-9 2018



For more information please visit the website at:
www.academic-conferences.org/conferences/iccws/

Although the call for papers has formally closed, late submissions can still be considered—particularly for presentations, workshops, round table discussions, and posters.

Early Bird Registration is available until 5 January 2018 and readers of The Cyber Defense Review can claim a 20% discount off the registration fee by quoting MKTP20 when prompted at checkout.

THE CYBER DEFENSE REVIEW

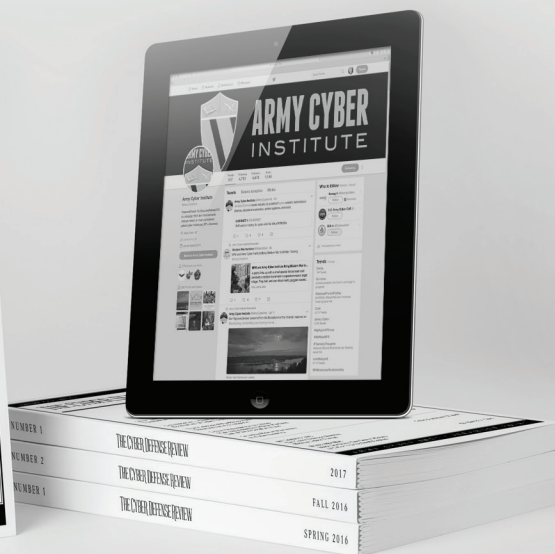
CONTINUE THE CONVERSATION ONLINE

 cyberdefensereview.army.mil

AND THROUGH SOCIAL MEDIA

 Facebook @army cyberinstitute

 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.