VOLUME 3 ◆ NUMBER 2 SUMMER 2018

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

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

SUBMISSIONS
The Cyber Defense Review welcomes submissions at
CDR Manuscript Central

WEBSITE
cyberdefensereview.army.mil

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

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

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

RESEARCH ARTICLES

BOOK REVIEW

The Cyber Defense Review

Introduction

VOLUME 3 • NUMBER 2

The Cyber Defense Review: Cyber Leadership During Uncertain Times

Colonel Andrew O. Hall

INTRODUCTION

During these uncertain times of relentless cyber onslaughts against critical US infrastructure and DoD networks and systems, cyber leadership has never been so important to effectively defend and manage the national cybersecurity ecosystem. The intensive and crippling nature of cyber conflict requires cyber leadership not only to defend against cyberattacks of significant consequence but to also generate integrated cyberspace effects in support of operational plans and contingency operations.

The summer edition of *The Cyber Defense Review (CDR)* marks the seventh issue of our scholarly journal, which features three leadership perspectives, a professional commentary, four research articles, and one book review. BG Kenneth Hubbard and MAJ Jared Nystrom discuss financial stewardship in the cyber ecosystem, while COL David Wallace and LTC Mark Visger address the use of weaponized "honeypots" under the customary international law of state responsibility. COL (Ret) Keith Tresh and Maxim Kovalsky provide their leadership perspective on California's Cybersecurity Integration Center and its advances in automated information sharing. Andy Cohen comments on effective cyber leadership, which stresses the importance of directing assumptions towards productive behavior. The *CDR* research articles address national workforce development for cybersecurity, best practices for teaching cybersecurity in small public universities, the consequences of state-sponsored hostile cyber operations under international law, and cybersecurity architectural analysis for complex cyber-physical systems. Finally, Dr. Jan Kallberg and Cadet Daniel Muncaster review *Strategic A2/AD*

Colonel Andrew O. Hall is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, Colonel Hall leads a 53 person multi-disciplinary research institute and serves as the Chairman of the Editorial Board for *The Cyber Defense Review* journal; and Conference Co-Chair for the International Conference on Cyber Conflict U.S. (CyCon U.S.). He has a B.S. in Computer Science from the USMA, an M.S. in Applied Mathematics from the Naval Postgraduate School, and a Ph.D. in Management Science from the University of Maryland. Colonel Hall additionally teaches in the Department of Mathematical Sciences and the Department of Electrical Engineering and Computer Science at the USMA. Since 1997, Colonel Hall's military career has been focused on operations research and solving the Army's most challenging problems using advanced analytic methods. Colonel Hall also serves as the President of the Military Applications Society of the Institute for Operations Research and the Management Sciences. His research interests include Military Operations Research, Cyber Education, Manpower Planning, and Mathematical Finance.

in Cyberspace, which details the growing importance of cyber capabilities to the global balance of power.

I am pleased to announce that in July, the *CDR* installed the ScholarOne Manuscript web-based system to integrate manuscript invitation, submission, file conversion, correspondence, tracking, reviewer management, decision making, reporting, and user data management. Further, this system also integrates our *CDR* print and online production. Along with the end-to-end, customizable workflow system, the *CDR* also gets the benefit of working with a qualified team of manuscript implementation, training, and support experts. Also, we are excited with the *CDR's* continued relationship with JSTOR and its Security Studies collection, which now reaches 8,000 institutions and libraries in 160 countries. While *CDR* articles and authors are on JSTOR, Google is busy indexing their work for the cyber community.

The next opportunity for our community of cyber researchers, scientists, teachers, practitioners, operators and leaders to meet, discuss, challenge, and explore future solutions within the cyber domain is the 2018 International Conference on Cyber Conflict U.S. (CyCon U.S.), which is a collaborative effort between the Army Cyber Institute at West Point and the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) will be held November 14-15, 2018 at the Ronald Reagan Building in Washington, D.C. As a venue for fresh ideas, relevant and actionable content, and insight into future trends, CyCon U.S. seeks to promote multidisciplinary cyber initiatives that advance research and cooperation on cyber threats and opportunities. To support this year's theme of "Cyber Conflict during Competition", the CyCon U.S. conference is seeking papers that speak to the combination of cyber, electronic and information operations that infiltrate systems

and infrastructure, influence the sentiments of the populace and national decision makers, destabilize partners and allies, and set conditions for a 'fait accompli' campaign with conventional forces. In addition, this year's CyCon U.S. conference marks the inaugural meeting of the world-class CDR Editorial Board. Please visit our ACI CyCon U.S. website for more information. Stay tuned for an impressive lineup of authors in the Fall CDR, to include GEN Joseph L. Votel, Commander of U.S. Central Command; Angela Messer and Brad Medairy, both senior cyber executives at Booz Allen Hamilton; Aristedes Mahairas, FBI Special Agent in Charge of the New York Special Operations and Cyber Division; Reva Goujon, Vice President of Global Analysis at Stratfor and Geopolitical Risk and Forecasting Expert. We look forward to continuing our dynamic, multidisciplinary dialogue on cyberspace.

The Cyber Defense Review

Senior Leader Perspective

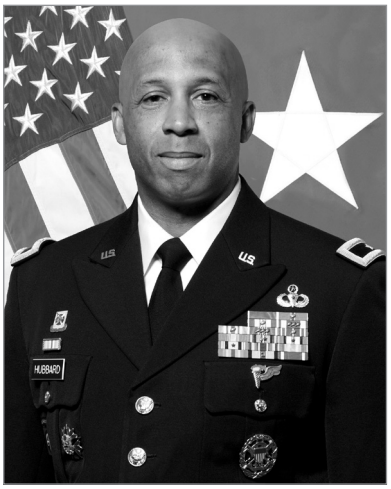
Financial Stewardship in the Land of "1's and 0's"

Brigadier General Kenneth D. Hubbard
Major Jared Nystrom

ABSTRACT

Budget processes supporting cyberspace operations are uniquely challenged due to their dispersal within Department of Defense (DoD) Services and agencies. This budgetary structure fails to provide the visibility needed to analyze and report on cyberspace investments. Furthermore, this structure fails to provide the resolution, with a high level of confidence, on how the DoD executes money in support of cyberspace operations. Establishing a budgetary process similar to that employed by special operations would synchronize and integrate funding activities to operational functions and tasks. This includes the creation of a cyberspace Major Force Program (MFP) that would provide cyberspace budget lines throughout the department. These proposals would create a budgetary structure that could best serve the unique requirements demanded in cyberspace. Doing so would act to acknowledge the cyberspace domain as a separate environment integrated across all Services.

The diffuse nature of the military cyber budget presents the Department of Defense (DoD) with a challenge for effective budgetary management; DoD must develop a new method for managing cross-program funding to improve mission effectiveness and achieve management efficiencies.[1] Cyberspace is not unique among warfighting domains in that operational readiness is dependent upon the timely execution of a balanced program of resources tied to valid requirements. The DoD budgetary structures have kept pace with the explosive growth in cyberspace; however, the resulting system fails to provide the visibility needed to analyze and report on cyberspace investments. Aligning cyberspace budgetary processes to better support operations would provide increased transparency and improve force readiness by synchronizing capability development across the DoD.



Brigadier General Kenneth D. Hubbard currently serves as Director of Resource Management for 3rd Army ARCENT G8, and previously served as the Director, Capability and Resource Integration J8, United States Cyber Command. He is the son of a career Army officer and a 1986 graduate of the South Carolina State Army ROTC Program. His assignments include the Director for Resource Management (G8), IMCOM; the Director of the Army Budget's Operations and Support Directorate; USFOR-A J8 while assigned as the V Corps G8, Operation Enduring Freedom, Afghanistan; Division G8 (Comptroller) for 1st Infantry Division; MNSTC-I G8, Operation Iraqi Freedom, Iraq; Contingency Operations Budget Analyst, Army Budget Office; and Defense Resource Manager, J8, Joint Chiefs of Staff. BG Hubbard is a graduate of the Industrial College of the Armed Forces and Air Command and Staff College. He holds graduate degrees from Syracuse University and the National Defense University.

Every DoD Service and agency submits an annual budget estimate in order to build the overall DoD budget, which is then provided as part of the President's Budget (PB) request to Congress.[2] This budget is a detailed forecast of the next two-year's financial execution developed in accordance with fiscal programming guidelines, as well as assessments of on-going programs.[3] It aligns with Congressional appropriations, and includes justifications to provide transparency regarding the investment of taxpayer dollars in defense programs. Programs within the defense budget are organized into Major Force Programs (MFP), which aggregate program elements that reflect a force or support mission and contain the resources necessary to achieve an objective or plan.[4] Currently, cyberspace operations are not organized within an MFP, with budget lines diffused within the financial records of individual Services and agencies. Budget analysts and staffers must manually correlate cyberspace efforts across multiple, disparate budget estimates to gain a basic understanding of how funds are being invested.

The lack of oversight of cyberspace resource planning, programming and budgeting have consistently been a contentious issue since the establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command. During the 2010 confirenate Armed Services Committee characterized this lack of oversight as well-known within the Federal Government.[5] Furthermore, the Congressional language during this time-period describes the issue as fragmented within the DoD, the executive branch as a whole, and within Congress.[6] Initial attempts to provide a unified budget drew upon authorities granted to the DoD Chief Information Officer (CIO) within the Information Technology Management Reform Act. Also known as the Clinger-Cohen Act,

Major Jared Nystrom is an Operations Research and Systems Analyst (ORSA) Officer assigned to J8, United States Cyber Command. He is a graduate of Tulane University ROTC where he received Bachelor's Degrees in Economics and Psychology and commissioned into Military Intelligence (MI) detailed to Armor. He previously served in both the 2nd and 14th Cavalry Regiments and commanded B Company, 532nd MI Battalion, Republic of Korea. He holds a Master's degree from the Air Force Institute of Technology (AFIT) and will return this fall to pursue a Ph.D. in Operations Research.

this legislation was signed into law as part of the 1996 National Defense Authorization Act (NDAA).[7] This law improved the methods used by all Federal agencies to acquire, use, and dispose of Information Technology (IT) by leveraging enterprise solutions,[8] and was later established in policy through the Office of Management and Budget Circular A-11.[9] The Clinger-Cohen Act charges the DoD CIO with the responsibility for reviewing and providing recommendations to the Secretary of Defense (SecDef) on budget requirements for IT and national security systems.[10] Although initially conceived to handle business operations IT, the authorities granted in the Clinger-Cohen Act were later attributed to cyberspace operations to include both offensive and defensive capabilities.[11] The current budgetary framework developed organically through this process. This extrapolation of authorities from business support IT to operational cyber mission forces results in a system ineffective in developing and providing oversight of a cyberspace budget across the Services and Joint Forces. This introduces potential risk to force readiness due to a lack of synchronization of development amongst Services, and the inability to function as a combined joint force.

A brief history of the US special operations offers insight into the effective application of military operations resourcing within a nascent command. The U.S. Special Operations Command (SOCOM) possesses unique Service-like authorities for funding and accounting. To explain this unprecedented authority, Charles G. Cogan provides a contemporary perspective as chief of the Near East and South Asia Division in the Directorate of Operations of the Central Intelligence Agency between mid-1979 and mid-1984.[12] Cogan assesses the capability gaps following the failure at "Desert

One" as well as the articulation of intent behind the Cohen-Nunn Act that consolidated Special Operations under SOCOM.[13] In April 1980, the United States military suffered a humiliating defeat during the failed attempt to rescue 53 Americans during the Iranian hostage crisis. The multiple setbacks at Dasht-e-Kavir, also known as "Desert One"[14] resulted in the failure of Operation *Eagle Claw,* and tragically the death of eight American service members.[15]

Following an internal investigation, chaired by Admiral James L. Holloway, the DoD established a Counterterrorist Joint Task Force (CTJTF) in 1980 as a field agency of the Joint Chiefs of Staff (JCS) to consolidate advocacy for special operations.[16] Congress later took a more significant role in the organization of Special Operations, culminating with the passage of Public Law (PL) 99-661 in 1986.[17] Section 1311 of this legislation adds Section 167, Title 10, which formally established SOCOM as a four-star unified command tasked to prepare special operations forces to carry out assigned missions.[18] Furthermore, this legislation directed the SecDef to appoint an Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SOLIC)), and create a new major force program (MFP) category 11 for the DoD Five-Year Defense Plan.[19] The Congress tasked the ASD(SO/LIC) to prepare and justify program recommendations for the newly minted MFP, and restricted the authority to the SecDef for any reprogramming of special forces operations.[20] Comparatively, the cyberspace domain requires this level of oversight and authority to properly execute resources.

The establishment of Special Operations Forces (SOF) MFP 11, managed by the AS (SO/LIC), provides clear traceability of resources from the Congress directly to the SOF community. Programs organized under an MFP allow a more precise articulation of investments, facilitating immediate identification of resources assigned to a particular activity or capability regardless of Service. Through this system, Congress can control funding to individual MFPs, allowing prioritization and preservation of joint capability and capacity during periods of budget scarcity.

The DoD should seek to optimize resourcing of cyberspace operations, versus the current CIO-driven model where each Service and agency resources and manages cyber capabilities independently. This current model results in a 'cottage industry' of cyberspace capabilities not only hindered by redundant efforts but also results in unaddressed capability gaps. The responsibilities given to DoD CIO to budget cybersecurity do not provide the controls or necessary authority to manage cyber resources. This responsibility results in DoD CIO attempting to report on what they believe the Services and agencies are spending on cybersecurity based upon loose reporting guidance and layers of independent organizational staff providing budget justifications.

The Office of the Under Secretary of Defense Comptroller (OUSD(C)) and the Office of the Secretary of Defense Cost Assessment and Program Evaluation (CAPE) are the two

primary offices at the OSD level for providing oversight of the DoD budget and the Program Objective Memorandum (POM). The OUSD(C) provides support to the DoD CIO through the Office of Investment Programs Directorate. This directorate oversees billion-dollar programs, but cyberspace requires funding for million-dollar programs, an order of magnitude less, making oversight of these programs a lower priority for the Investment Programs Directorate and OUSD(C). The CAPE has limited personnel dedicated to a cyberspace program across the five-year Fiscal Year Defense Program (FYDP). A dedicated office with a focus on relatively small appropriations may provide greater efficiencies. A more robust effort would assist DoD in long-range planning and programming of cyber requirements. In conjunction with the Principal Cyber Advisor (PCA), OSD Policy, CAPE could better align cyber functions, increase transparency, and synchronize efforts amongst the Services and optimize acquisition processes. This effort will create efficiencies and improve mission effectiveness.

This article offers the following recommendations towards improving cyberspace operations budgetary processes and management.

- Creation of a cyberspace MFP to ensure required resourcing is available to execute critical domain-specific missions, similar to the recognition of special operations. An MFP allows proper pairing of resources to requirements, facilitating a rapid pace of capability development required within cyberspace. An MFP provides the necessary transparency in cyberspace investments to Congress. Furthermore, an MFP protects resources intended for critical cyberspace capability and capacity during periods of budget scarcity, rather than risk diversion of those resources towards priorities internal to Services and agencies.
- Elevate the PCA to a comparable position to the Assistant Secretary of Defense in line with the roles and authorities for the ASD(SOLIC). The PCA should develop the annual and long-range strategic plan for cyberspace development. This also facilitates proper implementation and oversight of a cyber MFP, consolidated within an office armed with proper resource management and acquisition expertise. An elevated PCA also enables DoD CIO to focus exclusively on DoD's information enterprise and business IT solutions versus cyberspace operational capability, as was the original intent behind current policies.
- Cyberspace operations require a dedicated Joint Staff element to ensure the personnel readiness, policy, planning, and training of the Cyber Mission Force. This Joint Staff element would also act in a military advisory capacity for the PCA. Placing this capability within the Joint Staff facilitates coordination across all combatant commands, and allow better integration of cyberspace forces in support of Chairman of the Joint Chiefs of Staff priorities.

Under the current model, the DoD does not have the resolution to provide, with a high level of confidence, how money is being executed in support of cyberspace operations. We recommend creating a budgetary oversight process outside of CIO to improve clarity and control. If implemented, the recommendations in this paper would produce a budgetary structure that could best serve the unique requirements demanded in cyberspace. Doing so would acknowledge the cyberspace domain as a separate environment that is integrated across all Services. The ability to focus resources on the most critical cyber threats and provide the optimum solutions across all Services is necessary to derail future hazards.

NOTES

1. Ashton Carter, The Department of Defense Cyber Strategy. Washington D.C.: Department of Defense, 2015.

2. DoD Directive 7045.14. "The Planning, Programming, Budgeting, and Execution (PPBE) Process." Washington D.C.: Government Printing Office, 2013.

3. Ibid.

4. Defense Acquisition University. n.d., April 9, 2018, https://dap.dau.mil/glossary/pages/2192.aspx.

5. U.S. Senate. (2010). Nominations before the Senate Armed Services Committee, Second Session, 111th Congress. Washington D.C.: Government Publishing Office.

6. Ibid.

7. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

8. Ibid.

9. Office of Management and Budget (OMB) (2000). Circular A-11. Washington D.C.: Government Publishing Office.

10. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

11. DoD Manual 7000.14-R. (2015). DoD Financial Management Regulation Volume 2B. Washington D.C.: Government Publishing Office.

12. Charles Cogan, "Desert One and its disorders." The Journal of Military History 67, no. 1 (2003), 201.

13. Ibid.

14. Ibid., 211.

15. Ibid., 211.

16. Ibid., 214.

17. Ibid., 2151.

18. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

19. Ibid.

20. Ibid.

Toward Automated Information Sharing California –

Cybersecurity Integration Center's approach to improve on the traditional information sharing models

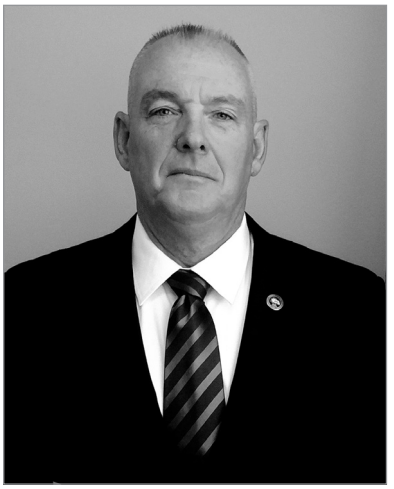
Keith Tresh
Maxim Kovalsky

INTRODUCTION

On August 31, 2015, California Governor Jerry Brown signed Executive Order B-34-15, directing the establishment of the California Cybersecurity Integration Center (Cal-CSIC). The new center operates under the auspices of the Office of Emergency Services (OES), with the California Department of Technology, California National Guard, and the California Highway Patrol acting as the key partners in the coordination of cybersecurity related activities within the State.

In his Executive Order, Governor Brown tasks the Cal-CSIC with two primary missions: facilitate information sharing across the state and coordinate statewide responses to cyber incidents. Given the increasing threat from cyberattacks to the State government and all California governments, businesses, and citizens, the Cal-CSIC's mandate is immediate action to mitigate those risks. It takes significant planning and time to coordinate an incident response capability for statewide deployment, therefore, the immediate focus is to create and implement a statewide information sharing program.

The team faced a critical decision: Should the Cal-CSIC adopt a unidirectional information sharing model whereby the primary product is human-readable and addresses common threats and vulnerabilities, or take advantage of the mandate and experiment with a unique approach? The authors of this paper argue that for cyber threat information sharing to be effective it must be crowd-sourced, where partners agree to share technical details about suspected intrusions with all other participants and done at machine speed. They also reflect on the lessons learned from their experience implementing such a program.



Keith Tresh was appointed as the commander of the California Cybersecurity Integration Center (Cal-CSIC) by Governor Jerry Brown on October 6, 2016. His office is part of the Governor's Office of Emergency Services.

A retired Army colonel, Mr. Tresh is also a veteran C-level IT management professional and an educator with a passion for information assurance and awareness. He served in the Army for more than 33 years, including a combat tour in Iraq from 2005-2006. Among his many assignments, he was the J6 for the California National Guard from November 2006 to June 2011.

Keith holds a Master of Science degree in Computer Information Systems from the University of Phoenix and a Master of Science in Strategic Studies from the Army War College. Mr. Tresh lives and works in Sacramento with his wife Coco and his children – Justine, 30, Austin, 24, Hunter, 22, and Kristina 18.

Given the decentralized nature of California state government networks, where each agency and department is responsible for managing—and securing—its infrastructure, historically, information about cyberattacks on one entity was not readily shared with other organizations. Before the establishment of the Cal-CSIC, there was not an organization positioned to share security information and expertise with all California governments, whether state, local, or municipal, higher education, utilities, and the private sector.

Cal-CSIC's unique value

The Cal-CSIC builds and expands upon the existing partnerships of the California State Threat Assessment Center (STAC) which is collocated with the Cal-CSIC.[1] In collaboration with federal agencies, fusion centers, local and municipal governments, and other information sharing organizations, the Cal-CSIC gains access to and disseminates information about existing and emerging cyber threats. While processing, analyzing, and disseminating information on opportunistic cyber threats to California entities was an important start, the Cal-CSIC acknowledged early on that it needed to produce actionable data and products.

Information that brings the most value to Cal-CSIC's partners reflects the threat's current posture, profile, and intent. This information is a "live broadcast" about cyber incidents that are unfolding across California. Given the Cal-CSIC's position at the intersection of federal and state government entities, it has the right resources to accomplish this ambitious goal. This "broadcast" enables the Cal-CSIC to develop an early warning system, where the collective can prevent attacks through the use of the data it gains from the first victim of the attack. Finally, to keep pace with the speed at which attackers change their infrastructure and techniques,

Maxim Kovalsky is a Senior Manager in Deloitte's Cyber Risk Advisory practice. With over ten years of experience in technology and cyber security, Maxim's work at Deloitte has focused on security intelligence and operations strategy and implementation projects across multiple sectors. He has led engagements in areas covering cyber security program assessments, threat monitoring and detection, cyber incident response, and threat intelligence.

Prior to joining Deloitte, Maxim directed cyber threat intelligence research at Flashpoint, where he supported clients in the healthcare, retail, and financial services sectors. Before that, Mr. Kovalsky worked for the Federal Bureau of Investigation, providing operational and intelligence support to complex cybercrime investigations. Mr. Kovalsky is a reservist in the US Army and a member of the Cyber Threat Fusion Cell within the Army Reserve Cyber Operations Group.

the Cal-CSIC has to process, correlate, and share information as close to machine speed as possible.

The added strategic benefit of an efficient sharing of tactical information requires the development of a holistic picture that describes the threat landscape facing a broad set of California entities. Understanding the threat holistically, as well as the trends in cyberattacks can allow state leaders and business owners to formulate a rational model for resource allocation.

Challenges with traditional information sharing models

At the beginning of the Cal-CSIC's development, a critical decision faced the team. Should the Cal-CSIC adopt a commonly implemented information sharing model where most of the burden to produce threat and vulnerability notifications rests with the center? To determine an answer to this question required an understanding of the challenges inherent in the traditional model and a new vision for how to improve. The following challenges were identified in the very early stages of planning and design of the Cal-CSIC's future state.

Alerts Take too Long to Produce. Given the speed at which attackers change tactics and infrastructure, production and dissemination of human-readable reports frequently result in the information recipient getting data that is no longer relevant or actionable. There is a benefit in detecting a previously unnoticed intrusion based on that information, but it has little preventative value.

Free Rider Problem. In addition to delays associated with manually sharing cyber threat data from an incident, the model is plagued by the free rider problem.[2] Stemming from economic theory, the free rider problem occurs when absent a precise definition or enforcement of rules, members of a

community use a public good or service without contribution. The problem is exacerbated when members decrease their contributions because they believe that others are riding free, which leads to the eventual depletion of that good. Voluntary and manual contributions in the context of information sharing suffer from a similar problem, wherein partners may be reluctant to share information due to resource constraints, or fear of appearing vulnerable.

Operationalization Challenges. Consumers of shared information frequently struggle to understand how it is relevant to their operating environment. The recipient grows weary after parsing so many notifications that do not apply to their agency. Unparsed cyber threat products often end up in email folders that are rarely checked. In addition to email fatigue, there are challenges associated with operationalizing information for those events that are deemed relevant. If the message contains an attachment with a list of threat indicators, for example, someone on the receiving end must be tasked with parsing out that data; someone else has to enter that data into reference lists for alerting or blocking within security technologies. Given the acute cybersecurity talent shortages within the public sector, the few resources capable of accomplishing those tasks are likely stretched too thin to take on additional responsibilities.

Lack of Trust. Participation in information sharing organizations is often hampered by the lack of trust of members in the conduit of shared information. Partnership candidates fear that the information shared by them will expose their organizational deficiencies or question their capabilities to defend against cyber threats with ramifications to influence over critical decisions, careers, budgets, and the projected image of the entity.

The envisioned solution

Solving for the four mentioned deficiencies above with traditional information sharing models requires the reduction of human involvement in the sharing, receipt, and actions taken on threat information. In other words, sharing information—both from center to the hubs, and from the hubs to the center—has to be as close to machine speed as possible. At its core, the model has to be supported by a technology that allows the Cal-CSIC to receive attack telemetry from partners, aggregate the relevant data, and disseminate it to threat detection and mitigation tools for automated ingest and action.

The envisioned solution architecture, depicted in Figure 1 below, started out with deploying a threat list integration server within the partners' network technology environment. This virtual machine pulls new threat indicators from the Cal-CSIC's threat intelligence cloud at periodic intervals and organizes the data by indicator type. The Security Event Information Management (SEIM) system is configured to ingest this data and alert security analysists of any positive correlations. In step 2 of this layer, potentially malicious events that meet Cal-CSIC's criteria are minimized to ensure that no attributable or personally

identifiable information leaves the agency, and are forwarded to a local security event collection server, which in turn, submits these events to the Cal-CSIC's security event reporting platform. Newly observed indicators are then shared with the rest of the partners through the threat intelligence platform, as depicted in step 6 of the diagram.

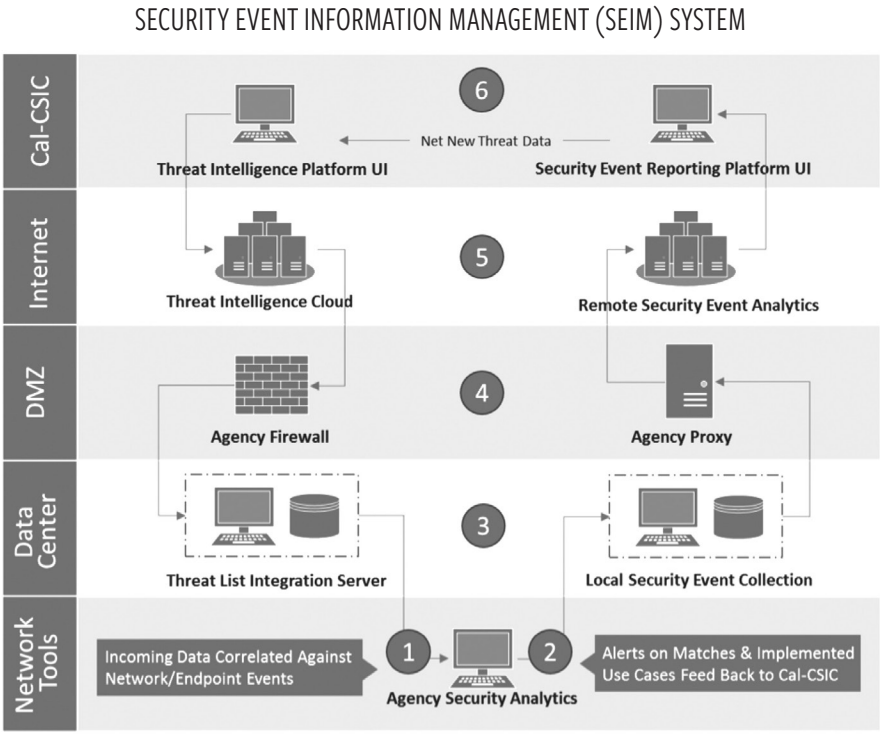


Figure 1. Solution Architecture

To alleviate the burdens associated with the initial integration, the Cal-CSIC provides direct support to partners to configure their threat detection and mitigation tools to leverage a common data model. This enables partners to alert on or block correlated internal events that are generated by the Cal-CSIC-shared data without additional human intervention.

Once the threat intelligence integration technology was implemented, the Cal-CSIC established unidirectional automation to share attack data out to partners. This process is depicted in step 1 of Figure 1. Unidirectional sharing dramatically enhances the speed at which attack data is shared and implemented for preventative and detective purposes. Automation also addresses the operationalization challenges because indicators are ingested directly into the security devices, relieving a human operator from the task of taking manual steps to act upon each portion of received data.

However, unidirectional indicator sharing has its limitations. It does not address the free rider problem nor the lack of trust. To overcome these challenges, the Cal-CSIC partners have to agree to abide by a set of core requirements to receive the benefit of the Cal-CSIC's crowd-sourced threat intelligence. Participation is always voluntary which strengthens the trust amongst participating members. Automation of the sharing process serves as an enforcement mechanism while increasing the speed at which other partners receive the valuable information.

The Cal-CSIC and its partners have a shared understanding of the model through clearly defined parameters of information that is subject to sharing through a common data model. Practically, this requires walking potential partners through the process and then formalizing the relationship by a mutually signed Memorandum of Understanding (MOU). To mitigate privacy concerns and protect civil liberties, the Cal-CSIC clearly defines the data elements: information attributable to a specific organization or its users is not shared with Cal-CSIC's other partners.

To support the common data model, the Cal-CSIC has a defined matrix of threat detection use cases and criticality ratings that contain information relevant to the Cal-CSIC partners. Each of the use cases requires a level of visibility into the environment necessary to detect the malicious activity in question. For example, to detect account sharing, which may indicate a compromise of credentials, the use case requires the collection and processing of Windows and Linux event logs. An example of this particular use case is shown in Figure 2 below. A roadmap for onboarding the necessary log sources is developed with each partner early in the onboarding process, and progress throughout onboarding is monitored.

ID	USE CASE NAME	USE CASE DESCRIPTION	ANTICIPATED LOG SOURCES	EXT IOC TYPE	BASE QUERY
TA-010	Potential account sharing detected from distinct source address	Detect and alert on internal apps and authentication to those apps for the same user, from different sources in X amount of time	WIN Logs (login events etc.) Server (WIN/UNIX) Asset (Office Information etc.)	N/A: All internal network events	Sourcetype= <windows_logs> | eventstats count (<src_ip>) as TotalSource by <UserID> | where TotalSource > <threshold>

Figure 2. Account Sharing Use Case

Once the threat detection use cases are deployed, and an alert is generated that meets the established criticality threshold of the relevant attack data and context, it is automatically forwarded to the Cal-CSIC. The Cal-CSIC then analyzes and shares this attack data back out to the partners which creates a multiplier effect where one partner's

successful detection of an attack can lead to prevention and detection across the other partner entities.

Testing the solution during a pilot

The Cal-CSIC's strategic goals are ambitious, and the Cal-CSIC understands that to pioneer an advanced information sharing model requires hiring able staff, developing the processes to onboard new partners, and deploying the information sharing technologies. The Cal-CSIC also appreciates that their operations cannot happen in a vacuum and that the integration model needs to be tested by partners for viability. As a result, the Cal-CSIC decided to develop its information sharing program through a pilot. Three partners, the California Department of Corrections and Rehabilitation, the Governor's Office of Emergency Services, and the California Franchise Tax Board participated in the six-month pilot and provided feedback throughout the process to enable the Cal-CSIC to get the program up and running while simultaneously identifying enhancement areas to facilitate future partner onboarding.

Several challenges were encountered early in the process. For information sharing to have value, the partner receiving the attack data must have security tools that are configured to accept and act upon the data. Once the Cal-CSIC began working directly with each partner on the technology integrations, it became clear that the Cal-CSIC would need to assist the partners to configure their existing threat detection technologies to both send and receive the relevant alert data. The Cal-CSIC has overcome this challenge by assigning a security engineer to work with each of the partners to implement new threat detection use cases or to enhance existing logic.

Valuable lessons were also learned from the perspective of relationship management and continual partner engagement. Initially, the Cal-CSIC sought an executive sponsor within each partner entity to drive the Cal-CSIC integration within their organization. However, throughout the pilot, the Cal-CSIC understood that the formal role of the leader who facilitated the Cal-CSIC integration was not the determining factor in the success of the integration. While it is important that the leader clearly communicates to the staff the benefits to the organization, when it comes to resource allocation to accomplish the required tasks, it is the involvement of middle management who champion the integration that assures the success of the partner onboarding. This is a valuable lesson learned because it demonstrates that either an executive or a middle manager can champion the Cal-CSIC integration. This enhances the scalability of the Cal-CSIC because middle managers are often closer to the resources and security tools than executives, and can personally conduct or oversee the integration.

Opportunities for improvement

As the Cal-CSIC moved from planning, to pilot, to the operationalization of the program it has identified several areas for improvement across the state's security posture and

within the Cal-CSIC. Through a series of conversations with potential partners, it became clear that many state entities perceive emerging security technologies as the panacea to cybersecurity risks. Advanced security tools, however, often provide little value when deployed with default configurations. They require a team of professionals with security engineering skills to continuously configure and customize these tools to both reflect the reality of the local environment and the dynamics of the threat landscape.

The Cal-CSIC also observed that the model deployed during the pilot is useful for entities with existing Information Technology and security programs, and ones that have visibility into their respective environments. However, it would not be effective for an entity that had little to no visibility or security infrastructure to consume the shared information. For these entities, the Cal-CSIC recognizes that an alternative model is required. This additional model entails the Cal-CSIC deploying and managing sensors at the partner entity.

Finally, as the Cal-CSIC scales to incorporate partners from across local and state agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations it is clear that the volume of data that the Cal-CSIC will ingest and share will require a big data processing platform. The scale of the Cal-CSIC's technology stack must match the scope of the Cal-CSIC's mission. Additionally, the Cal-CSIC must implement further automation and data analytics that will enable rapid analysis of the received security data.

CONCLUSION

An information sharing model that is easy to implement is likely ineffective. Although automatic bidirectional information sharing requires more time and expertise on the front-end than in a traditional information sharing model, it creates sharing mechanisms that are both more responsive to today's threat landscape, and are more effective in preventing and detecting those threats. These benefits are multiplied by the speed at which this information can now be shared, which imposes high costs on the attackers by rendering the staging infrastructure useless in a brief period.

The authors of this paper do not argue that while the Cal-CSIC's approach was unique in the state government sector, it is not the only model to effectively counter emerging cyber threats. Other states, for example, have moved down the path of consolidating networks into an enterprise environment to gain direct visibility into malicious events at the asset level, rendering technical information sharing superfluous.

For other state governments operating with a federated organizational structure similar to California's, the Cal-CSIC's pilot demonstrates the feasibility of leveraging bidirectional information sharing to increase the cybersecurity posture of the state as a whole.

NOTES

1. “State Threat Assessment Center,” Governor’s Office of Emergency Services, http://www.caloes.ca.gov/cal-oes-divisions/state-threat-assessment-center, accessed on May 10, 2018.

2. Russell Hardin, "The Free Rider Problem" The Stanford Encyclopedia of Philosophy, May 21, 2003.

The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility

Colonel David Wallace
Lieutenant Colonel Mark Visger

Colonel David A. Wallace and Lieutenant Colonel Mark Visger[1]

The overarching aim of computer security is to reduce or eliminate risks to an organization's computer networks and cyber infrastructure. One increasingly common way cybersecurity professionals are defending their networks is through the use of so-called "honeypots". The term honeypot has come to mean a deception technique to defend computer systems against malicious operations. Generally, it is an information system resource whose value lies in its unauthorized or illicit use by a hacker. In essence, it is a virtual sting operation. Honeypots can also be weaponized. That is, a honeypot includes files that contain malware that, once exfiltrated by intruders, will cause significant damage and disruption to the intruders' computer networks. The legal issues associated with the use of weaponized honeypots under international law are complex, multi-faceted, and unsettled. This article investigates the legality of using weaponized honeypots under the international law of State responsibility. More specifically, the precise issue addressed is whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility? Ultimately, the answer to the question is "it depends" on the facts and circumstances of a given situation. However, as the analysis below shows, a State should proceed with caution before employing them.

I. INTRODUCTION

When most people think of "honeypots," they picture a plump Winnie-the-Pooh adorably getting stuck while trying to get honey out of a jug—a honeypot. In recent years, the term "honeypot" has migrated to the lexicon of cyberspace and operations. In the rapidly evolving realities of

computer security, the term "honeypot" has come to mean:

> [a] deception technique in which a person seeking to defend computer systems against malicious cyber operations uses a physical or virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment, having the intruders waste resources on the decoy environment, gathering counter-intelligence about the intruders' intent, identity, and means and methods of cyber operations. Typically, the honeypot is co-resident with the actual systems the intruder wishes to target. [2]

Honeypots can be multiple resources such as servers, laptops, web-facing applications or other technological ploys established to monitor and record the actions of cyber intruders. [3] Honeypots are deployed in various ways to make them attractive for hackers. In some cases, they appear to be the "crown jewels" of an organization such as intellectual property, operational plans or financial reports. Intuitively, to be effective, the honeypot must appear realistic. If it looks or feels fake in any way, intruders' suspicions will be raised, and the honeypot will not be effective. [4] In essence, it is a virtual sting operation. [5] Honeypots can also be weaponized. That is, a weaponized honeypot includes files that contain malware that, once exfiltrated by intruders, will cause significant damage and disruption to the intruders' own computer networks. [6] The following example illustrates the use of honeypots to protect critical infrastructure.

Suppose multiple international computer intruders have increasingly attempted intrusions into the computer systems of a large urban water management utility in the United States. The pernicious and persistent hackers have compromised the utility's data historian that manages information from the supervisory control and data acquisition infrastructure network. Such computer operations against the city's water infrastructure are more than just an inconvenience or distraction. More specifically, the intruders have created a real and looming threat because they may be in a position, at some point soon, to shut down water pumps, gates, and valves around the city allowing raw sewage to be dumped into the local waterways as well as creating sewage back-ups around the city. [7] Computer security experts hired by the water utility decide to set a trap to catch the hackers red-handed. They establish three different honeypots which are carefully designed so the intruders will think that they have discovered a computer which controls the physical settings on the water system. The honeypots have fake files, icons, and special security monitoring beacons, making it possible to closely track and observe exactly what the hackers are doing and attempting to do in the network systems. [8] Additionally, the honeypots are weaponized. Destructive malware is incorporated into the honeypots and, upon activation, will cause significant damage to an intruder's own cyber infrastructure.

The legal issues associated with the use of weaponized honeypots under international law are complex, multi-faceted, and unsettled. For legal advisors, policymakers, and academics among others, an outstanding starting point for considering such an important legal

Colonel David Wallace is Professor and Head, Department of Law, United States Military Academy, West Point, New York. In addition to his assignment at West Point, he has also served as a Deputy Staff Judge Advocate; Assistant/Associate Professor at the Judge Advocate General's School of the Army; Trial Attorney, Contract Appeals Division, United States Army Legal Service Agency; Trial Counsel and Legal Assistance Attorney, 3rd Infantry Division; and Public/Civil Affairs Officer, 81st Infantry Brigade. Colonel Wallace teaches a course in the Law of Armed Conflict. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia.

topic as the use of honeypots under international law has already been created, the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* This work analyzes the question of honeypots directly and indirectly as well as many other important topics spanning public international law in its nearly 600 pages of highly informative and influential text. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) invited an independent group of experts to produce the manual.[9] It is important to note that experts were limiting themselves to an objective restatement of the *lex lata* or law as it exists. They scrupulously avoided including statements reflecting the *lex ferenda* or what the law should be.[10] This article investigates the legality of using weaponized honeypots under the international law of State responsibility. Looking at the use of weaponized honeypots under domestic law or in the context of an armed conflict under international humanitarian law is beyond the scope of this article.

II. WEAPONIZED HONEYPOTS: AN ANALYSIS UNDER THE LAW OF STATE RESPONSIBILITY

The precise legal issue addressed in this section is whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility.[11] The law of State or international responsibility, which undeniably extends to cyber activities, "plays a central role in international law, functioning as a general law of wrongs that governs when an international obligation is breached, the consequences that flow from a breach, and who is able to invoke those consequences (and how)."[12] As a threshold matter, under the law of State responsibility, every internationally wrongful act of a State (usually acting through agents of the State) entails the international responsibility of that State.[13] An internationally wrongful act by

Lieutenant Colonel Mark Visger is an Assistant Professor in the Department of Law, United States Military Academy, West Point, New York. In addition to his assignment at West Point, he has also served as Staff Judge Advocate, First Army Division West; Chief, Rule of Law, Multi-National Corps, Iraq; Officer-in Charge, Bamberg Law Center; Government Appellate Counsel; Litigation Attorney, Trial Counsel Assistance Program; Senior Defense Counsel, Fort Rucker, Alabama; Chief, International and Operational Law, Tuzla, Bosnia-Herzegovina; Trial Counsel and Legal Assistance Attorney, 10th Mountain Division (Light Infantry). He is also CompTIA Network+ and Security+ certified. While at West Point, Lieutenant Colonel Visger has taught courses in Cyber Law, National Security Law, International Law and Constitutional and Military Law.

a State occurs when (1) conduct consisting of an action or omission is attributable to the State under international law; and which (2) constitutes a breach of an international obligation of the State.[14] An internationally wrongful act may be a violation of a State's treaty obligations, customary international law, or a general principle of law.[15] Before proceeding with a substantive legal analysis, it is important to note that these rules may seem archaic and ill-suited to the world of cyber-operations. However, customary international law is dependent on State practice. As state practice evolves, a different legal framework for cyber operations may emerge. For now, this analysis reflects the current customary law.

To begin the analysis, one must assess whether the delivery of malware via a honeypot to an attacking State would constitute a breach of an international obligation of the defending State. This analysis would depend upon the effects that the malware creates. If the effects are significant enough, they might be considered a violation of sovereignty, a violation of the rule against non-intervention, or possibly a use of force in violation of the UN Charter. For example, suppose the destructive malware contained in the weaponized honeypot spreads uncontrollably, infecting innocent third parties. If it was reasonably foreseeable that the destructive malware in the weaponized honeypot could and would spread to unintended targets, then the defending State that created and used it bears the responsibility for its internationally wrongful acts. On the other hand, malware that merely identified parties responsible for accessing the honeypot or tracks their activities may not violate international law.

The most likely scenario in the case of malware delivered via a weaponized honey pot would be that the delivery of such malware would violate the

sovereignty of another State, which is considered an internationally wrongful act.[16] The term or concept of sovereignty may be used as a synonym for independence, which is an essential element in being a State.[17] In the often-cited *Island of Palmas* arbitral award decision, the court defined sovereignty as "[i]ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[18] The principle of sovereignty is widely considered to be a primary rule of customary international law, which imposes an obligation on States to respect the inviolability of other States territories.[19] Most assuredly, the principle of sovereignty would encompass cyber infrastructure located in a State's territory.[20] The exact legal character of remote cyber operations by one State on another State's territory is unsettled in international law. However, if physical damage or loss of functionality results from such a remote cyber operation, it would be likely be considered a breach of sovereignty and thus an internationally wrongful act.[21]

If the delivery of the malware through a honeypot constitutes an internationally wrongful act, the responsible State must either provide a legal justification for its acts or it will be responsible under the rules for State responsibility.[22] If there is no legal justification, the State responsible for the internationally wrongful act is under an obligation to cease that act and offer appropriate assurance and guarantees of non-repetition.[23] Additionally, the State responsible for the internationally wrongful act must make full reparations to the injured State.

Possible Legal Defences for Perpetrators of Weaponized Honeypot.

Assuming the malware was significant enough to constitute an internationally wrongful act, the State utilizing a weaponized honeypot may be able to defend the legality of its actions on several grounds. This article will examine each ground in descending order of plausibility.

1. The first possibility is that the defending State did not commit an affirmative act at all, the delivery of the malware was accomplished by the intruding State accessing the honeypot and downloading the infected files. This possibility is addressed by *Tallinn 2.0*, and a majority of the experts concurred with this approach.[25] They contended that the State that accessed the honeypot and then exfiltrated the destructive malware contained within the stolen files is responsible for the damage it brought on itself. More specifically, the defending State that laid the trap did not conduct the actual activity causing the harm.[26] This view does not necessarily lead to the commission of an internationally wrongful act by anyone. The minority, on the other hand, believed that the defending State that placed the destructive malware files in honeypots set everything in motion which culminated, as anticipated, in the damage to the other State's computer system(s)[27] These experts opined that such an operation, at a minimum, violates the sovereignty of the targeted State thus committing an internationally wrongful act, assuming a severe-enough

effect from the malware. Note that this logic would not apply to a situation where malware is transmitted automatically upon access to the honeypot site and which did not require the affirmative step of transmitting purloined files.

The fact that the experts are divided in their analysis highlights the complexities of this issue and the complexities of applying extant international law to this subject. Viscerally, the majority's position rings true and is quite appealing. Namely, it is the intruding State that engaged in a remote cyber operation into the computer networks of the defending State. Moreover, is it not reasonable for a State defending its cyber infrastructure to take measures, like using honeypots, to protect itself against such intrusions and, quite frankly, deter others? Is it wrong for a State to use a dynamic, penalty-based form of deterrence? The law, as it is currently structured, does not address these questions.

2. The next possible justification would be that malware delivered via a honeypot would constitute a valid countermeasure. Countermeasures involve acts that would otherwise be unlawful but are executed as a self-help remedy intended to respond to an unlawful act.[28] The purpose of countermeasures under the law of State responsibility is to cause the breaching State to cease its unlawful actions or omissions, not to retaliate for the previous violation.[29] This is, quite literally, a situation where two wrongs are intended to make a right. Not surprisingly, there are limitations on the use of countermeasures, and a State seeking to use this legal doctrine must craft its weaponized honeypot accordingly.

Before the State operating the weaponized honeypot can claim that their actions are justified countermeasures, it is necessary to consider whether an intruding State committed an internationally wrongful act by engaging in a remote cyber operation in the first place. The answer is, not necessarily. For example, suppose an intruding State is engaging in cyber espionage. Cyber espionage refers to acts undertaken clandestinely or under false pretences that use cyber capabilities to gather or attempt to gather information.[30] Cyber espionage by States does not *per se* violate customary international law.[31] However, the method by which it is carried out *may* constitute a violation of international law such as a violation of the principles of sovereignty or non-intervention.[32] Under this scenario, the method used by the intruding State to engage in mere cyber espionage very well might not violate international law, and thus countermeasures would not be justified.

Another significant limitation to utilizing countermeasures is that they can only be used in response to State-sponsored cyber operations that are attributable to a State under the rules of State responsibility. As a result, a private individual or hacktivist group, operating independent of a State, cannot be subject to countermeasures.[33] The purpose of international law is to govern State-to-State interactions, and the international law doctrine of countermeasures would not apply to non-state actors. This doctrine has one small exception, as States are under a duty of due diligence to prevent cyber-infrastructure within their sovereign control from being used to violate the sovereignty of another state.[34] If the State from which the attack is emanating fails to exercise due diligence,

then the State utilizing a weaponized honeypot might be able to argue that countermeasures against the individuals responsible for the attack are justified.

Assuming that one can establish that the intruding State violated international law during its cyber intrusion, a weaponized countermeasure might be valid, although there are additional requirements to consider. In such a situation, it would be necessary to delve further into the legal requirements of countermeasures to assess whether a weaponized honeypot could be justified as a countermeasure. A State utilizing a weaponized honeypot would have to show that: (1) the damage or destruction caused by the weaponized files is commensurate with the initial internationally wrongful act; (2) that the purpose of the countermeasures is to induce the intruding State to comply with its obligations; (3) that the countermeasures do not affect other obligations such as the protection of fundamental human rights and universal norms; and (4) the State engaging in countermeasures must place the offending State on notice that it is doing so and offer to negotiate.[35] It would likely be challenging to comply with this last procedural condition of notice and an opportunity to negotiate. Suppose the defending State posted an information banner for its networks warning any users or intruders of the possible use of weaponized honeypots. Would that meet the notice requirement? In sum, subject to the comments above, the use of weaponized honeypots as a potential countermeasure cannot be rejected out of hand, although there are significant hurdles to be crossed before a State could legitimately claim that a weaponized honeypot was a legitimate countermeasure.

This review of the doctrine of countermeasures shows that use of this doctrine is difficult in a situation involving highly automated processes, which would likely be the case. The doctrine requires case-by-case legal analysis and is not conducive to an automatic process that delivers malware when triggered in a honeypot. The best possibility to ensure compliance would be to include the malware within files that are designed to be exfiltrated, and then rely on the argument that the attacking State (or private individual) was responsible for downloading the malware (although utilizing automatic delivery of the malware upon accessing the honeypot would likely be much more effective from the defending State's perspective). Regardless, justifying what would otherwise be an internationally-wrongful act under this legal theory contains many pitfalls and would need to be closely monitored.

3. While the doctrine of countermeasures has substantial legal requirements in execution, the doctrine of necessity is much more flexible but has a much higher threshold before it may be utilized. *Tallinn 2.0* succinctly defines the doctrine as: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[36] By its terms, a State claiming necessity must demonstrate: (1) a grave peril; (2) an imminent peril; (3) to an essential interest; and (4) the action taken is the sole means of safeguarding that vital interest from the grave and imminent peril.

While this threshold might be high, the State acting under a legal basis of necessity faces significantly less procedural obstacles due to the nature of the threat. First, the triggering act does not necessarily have to be an internationally wrongful act.[37] Similarly, third parties and non-state actors may be adversely affected by the action under a necessity justification without consequence.[38] Similarly, attributing the intrusion is not required, all that is required is a showing that the intrusion posed a grave and imminent peril to a vital interest and that the action taken was the sole means of safeguarding that interest.[39] This necessity framework may very well be a State's best legal justification for a weaponized honeypot, assuming the requisite threat has been established.

4. The final possibility for justification for a weaponized honeypot that otherwise violates international law is the State's inherent right to self-defence. Codified in Article 51 of the UN Charter, this provision recognizes that a State has "the inherent right of individual or collective self-defence if an armed attack occurs."[40] *Tallinn 2.0* recognizes that cyber operations might rise to the level of an armed attack.[41] Cyber operations could qualify as an armed attack if its "scale and effects" are comparable to that of an armed attack, Tallinn 2.0 provides a helpful framework to analyze whether such a cyber operation constitutes an armed attack.[42] The right to self-defence would justify weaponized honeypots that might otherwise be themselves considered a use of force in violation of the UN Charter. However, actions taken in self-defence must be limited to those necessary to repel the attack and proportionate to the attack and must cease when the attack is complete.[43] This justification would only apply in extreme situations, and likely not applicable to the typical weaponized honeypot.

III. CONCLUSION

As the analysis above demonstrates, the use of weaponized honeypots raises many challenging and complex legal issues under the law of State responsibility. This was also evident in the fact that the experts who wrote *Tallinn Manual 2.0* were split in their analysis. Ultimately, the answer to the question of whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility is "it depends" on the facts and circumstances of a given situation. However, as the analysis above shows, a State should proceed with caution before employing them.

NOTES

1. Colonel Wallace is the Professor and Head, Department of Law, United States Military Academy. Colonel Wallace teaches a course in the Law of Armed Conflict. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Colonel Wallace would like to thank the NATO CCDCOE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship. Lieutenant Colonel Mark Visger is an Assistant Professor of Law, Department of Law, United States Military Academy. He teaches courses in Cyber Law, International Law, National Security Law, and Constitutional and Military Law. The opinions in this article are those of the author and are not intended to reflect those of the U.S. Army, the United States Military Academy, NATO or the CCDCOE.

2. NATO Cooperative Cyber Defence Centre of Excellence *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Michael N. Schmitt, ed. (Cambridge: Cambridge University Press, 2017), 565. When multiple honeypots are used at the same time to create a virtual environment to deceive an intruder, the term "honeynet" is often used to describe such a design.

3. Tari Schreider, "Honeypots & Cyber Deception," *CISO Series on Today's Critical Issues* (March 2017): 2, https://ciso.eccouncil.org/wp-content/uploads/2017/06/Honeypots-Cyber-Deception.pdf.

4. Edward G. Amoroso, *Cyber security* (Summit, NJ: Silicon Press, 2007), 153.

5. Ibid., 154.

6. NATO, *supra* note 2, 174.

7. Tyson Macaulay, *Critical infrastructure: Understanding its component parts, vulnerabilities, operating risks, and interdependencies* (Boca Raton, FL: CRC, 2009), 295.

8. Tom Simonite, "Honeypots Lure Industrial Hackers Into the Open," *MIT Technology Review* (May 8, 2013), np. https://www.technologyreview.com/s/514216/honeypots-lure-industrial-hackers-into-the-open/. This hypothetical is based, in part, on a research effort done by security researcher Kyle Wilhoit.

9. *Tallinn Manual 2.0* is the second cyber law manual produced at the invitation of NATO CCD COE. The first was published in 2013 and focused on the international law governing cyber warfare.

10. NATO, *supra* note 2, 3.

11. NATO, *supra* note 2, 79-80. The customary international law of State responsibility is largely reflected in the International Law Commission's Articles on State Responsibility. This body of law consist of secondary rules of international law. Primary rules set forth international legal obligations. If primary rules are breached, it results in State responsibility. By contrast, secondary rules provide the general conditions for State responsibility and the consequences that flow from breaching primary rules.

12. Silvia Borelli, "State Responsibility in International Law," *International Law - Oxford Bibliographies* (Oxford: Oxford Press January 4, 2018), DOI: 10.1093/OBO/9780199796953-0031.

13. James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge: Cambridge University Press, 2007), 61.

14. Ibid, Art. 2.

15. NATO, supra note 2, 84.

16. Ibid., 17.

17. Ian Brownlie, *Principles of public international law* (Oxford: Clarendon Press, 1987), 80.

18. NATO, *supra* note 2, 84 citing *Island of Palmas* arbitral award, 838.

19.Michael N. Schmitt & Liis Vihul. "Respect for Sovereignty in Cyberspace." *Texas Law Review,* 95, no. 7 (2017), 1649.

20. NATO, *supra* note 2, 18.

21. Ibid., 20.

22. Ibid., 104.

23. Crawford, *supra* note 13, 196.

24. NATO, Ibid., 201.

NOTES

25. Ibid., 174
26. Ibid.
27. Ibid.
28. Ibid.
29. Ibid., 116.
30. Ibid., 168.
31. Ibid.
32. Ibid., 168-70.
33. Ibid., 113.
34. Ibid., 30.
35. Ibid., 111-134.
36. Ibid., 135.
37. Ibid., 137.
38. Ibid.
39. Ibid., 138.
40. United Nations, *Charter of the United Nations* (1 U.N.T.S. XVI, 1947), Article 51.
41. NATO, *supra* note 2, 339.
42. Ibid., 340-342.
43. Ibid., 348.

The Cyber Defense Review

Professional Commentary

Effective Cyber Leadership: Avoiding The Tuna Fish Effect and Other Dangerous Assumptions

Andy Cohen

There is a joke in Hollywood that goes something like this:

God informed Mother Teresa that he would like to grant her anything she wished for all the wonderful work she had done.

"Would you like your own house?" he asked.

"I have lived my whole life without one. Got along fine. No thanks," she responded.

"How about money?" God offered.

"Never needed money," she answered.

"Isn't there anything you'd like that I can give you?" he asked in frustration.

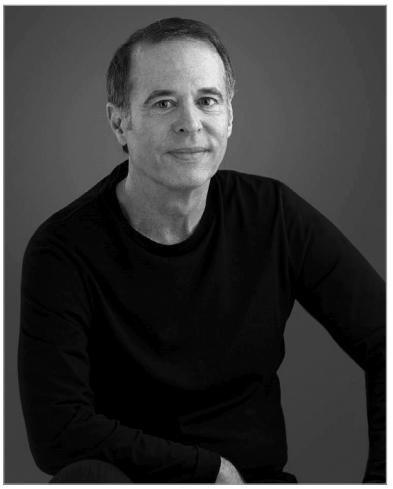
"Well, there is one thing," replied Mother Teresa.

"Name it," God said excitedly.

Shyly, she responded, "I'd like to direct."

When I owned my advertising agency, I too got the opportunity to pursue a dream of directing. In this case, it was for an advertising commercial, and it taught me a leadership lesson I will never forget.

We had been shooting for hours when my producer pulled me over and said we needed to take a half-hour break. "The crew needs it, and it's Union rules," he informed me. My assumption was that a break wasn't necessary and that with the right inspiration, the crew could finish up shortly, saving us money. So, ignoring the advice of the producer, I pulled the entire crew together and gave them what I felt was a highly motivational speech about how great they were doing, how I believed they were up for the challenge, and how if we pulled our energies together, we could finish up shortly.



Andy Cohen is an entrepreneur, best-selling author, and international AI/Cybersecurity Behaviorist. His TEDx talks and workshops are world-renowned and include appearances at The Army Cyber Institute Conference, Google, HSBC China, and The World Bank. He has a degree in experimental psychology and a room full of esteemed advertising awards for finding creative solutions that drive measurable sales. Andy is the Chief Assumption Officer of Andy Cohen Worldwide, a global advisory firm helping organizations make faster, better decisions and enhance critical thinking. Between engagements, Andy teaches at the world's most respected universities. Colonel (Ret.) Greg Conti, Ph.D. called Andy's new book, *Challenge Your Assumptions, Change Your World,* "a must-read for the security professional." *Follow the Other Hand,* Andy's first book, was a *New York Times* notable read and has been translated into multiple languages.

Four hours later, we were still shooting. It was a disaster. By ignoring my producer's advice, I ended up with an angry and tired crew whom I paid time and a half, eating thousands of extra dollars out of our budget.

Leadership Is About Directing People

Leadership is all about motivating people to march in particular ways that achieve desired results. To do so effectively, however, we must admit that sometimes we assume the world thinks just like ourselves and shares the same motivations. As a result, we can lack the patience, empathy, and/or sensitivity to listen to what others who are closer to the problem have to say. Our assumptions driving "a win" often move us further from the solution instead of bringing us closer to the answers we seek.

The following cyber case illustrates this point. Due to the sensitive nature of this story, it will be told in general terms to protect those involved. Essentially, about thirty FBI and U.S. Postal Inspection Service (USPIS) agents were assigned to investigate the 2001 anthrax attacks: code name "Amerithrax."

The investigators included a team of FBI agents and analysts tasked with the job of reviewing info bytes in the billions. For example, the bureau executed multiple search warrants and seized several computers and storage devices. A copy of the hard drives and storage devices was placed onto 2–3 stand-alone computers at the Washington Field Office (WFO). If you sat at one of the computers, you could browse a set of folders named something like the following:

- John Doe's desktop
- John Doe's laptop
- Laptop from John Doe's closet
- Girlfriend's laptop

If you opened one of those folders, you would see a folder labeled "C," and then if you opened the "C" folder, you would see a logical, recursive copy of the actual folders and files from the C: drive of the corresponding computer. This process was time-consuming and proved redundant in tracking info.

Therefore, a program called "Quincy" was employed to decode hundreds of file formats and visually (or audibly) present the data to an analyst. What is important to note is that the analyst needed only to look at the pages for each file and press one key per page: N for *not relevant,* R for *relevant,* or the space bar for *undecided.*

Still, as efficient as Quincy was, it would take the agents "hundreds of years" to manually review all the digital evidence. Therefore, it was proposed that certain "nonessential" data be reviewed programmatically using specialized tools instead of manually by agents. When this alternative was presented to the FBI Special Agent in Charge of this investigation, he responded that the director would not allow any "shortcuts" as this was the FBI's most important case.

It may have been that the FBI agent in charge did not communicate this challenge clearly enough. Or perhaps the director didn't ask for further clarification. Regardless of who was responsible for communicating or understanding the information, this unrealistic demand hindered motivation and generated the opposite of what it was meant to achieve.

Generating the "Tuna Fish Effect"

Here is what was described to me by one of the agents working on the case:

> A short time later, after the director negated the programmatic approach, I observed an agent sitting at the Quincy machines. He had stepped up the pace at which he was *reviewing* the data by pressing the N key every 1–2 seconds. This pushed the upper limits of the speed at which he could review the data accurately. A short time later, the same agent was pressing the N key about four times per second. That is, he was no longer reviewing the data—he was marking the data not relevant as quickly as he could.
>
> Later I returned and found the agent was no longer sitting in front of the computer. He had left, but he had placed a tuna can on top of the N key, which was marking countless pages of data *not relevant.*

For this article, we will refer to this behavior as the "Tuna Fish Effect": a negative organizational behavior resulting from a leadership direction based on an unrealistic demand, especially when it lacks clarification.

In essence, when leaders look for data that supports their assumptions versus acknowledging data that may contradict their assumptions, ineffective behavior follows. The leader runs the risk of misreading the situation, which directs energy away from solving the

problem and instead encourages unproductive behavior that's generated by an unrealistic demand. In your mind, you are absolutely making the right decision (but at the expense of generating the wrong results).

Cybersecurity Is Complex, Layered, and Confusing to Everyone

Cybersecurity represents an idea that is so complex and layered that as author Alexander Klimburg observed in *The Darkening Web: The War for Cyberspace,* we can't even agree if the term is one word or two. As leaders, we assume that admitting there are many cyber issues we do not know or understand is a bad thing, as it weakens our position. Instead, if we reject that assumption, we expand our decision-making capabilities to better manage this complex beast.

Raising our radars to identify and manage our assumptions does not ensure we will always make the right decisions, but it does decrease the odds of our making the wrong ones. When an FBI director inferred that "no stone be unturned," he might have been saying that, "I am the boss, and nothing will get overlooked on my watch" or, perhaps, "This is pretty complex stuff, so we better cover everything since I am not sure what we should cover." These desired outcomes are understandable but assume that a.) you alone as the leader make the difference, b.) no one knows better than you do how to solve the problem, and c.) I may not be an expert in this, but I am an expert at generating results.

We have all made these assumptions as leaders and upon reflection can probably identify how they created the Tuna Fish Effect.

The purpose of this article isn't to diminish your leadership skills but rather to propose a way to strengthen them. In a world of cyber complexity, it pays to encourage both yourself and your teams to identify those beliefs on all levels, from coding to budgeting. When these beliefs are taken at face value, such as "algorithms don't make assumptions," they have the potential to thwart your best intentions by directing energies in the opposite direction than was intended.

Since most assumptions are made subconsciously, I have included a few of the key ones that might be worth reviewing and discussing with your teams.

What Is Said = What Is Being Assumed: A List Of AI And Cyber Assumptions

- I put my best people on the job = A skilled Army captain can investigate computer crimes without any computer experience
- We are keeping the enemy out = Malicious attacks come from outside the organization
- This is good code = I don't have the time to double-check its accuracy
- We have the superior technology = No one can do what we can do
- Follow the algorithm = Algorithms don't make assumptions

- Biometrics are better than passwords = Fingerprints can't be lifted easily
- We are not a target = We are too small for anyone to care about and hack
- Cybersecurity is too complicated to understand = I'll leave it to others to figure out
- The government will protect us = The government is technologically superior
- My ISP protects my organization = Those in charge know what they are doing

The goal of discussing these assumptions is to direct your organization to think differently while minimizing the constrained thinking that leads to nonproductive behaviors.

Perhaps a good time to do this is over lunch, but maybe you want to leave out the tuna fish.

The Cyber Defense Review

Research Articles

Cybersecurity for the Nation: Workforce Development

Lieutenant Colonel Karen J. Dill

ABSTRACT

Cyberspace "is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." [1] It is the newest military domain affecting the Operating Environment (OE) and the focus of concern by the President of the United States. In the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, President Trump directed the Department of Defense and other agencies across the whole of government to identify a long-term way ahead to address education and retention of cybersecurity professionals. [2] There are two potential programs Chemical, Biological, Radiological, Nuclear (CBRN) Response Enterprise (CRE) [3] and the Civil Air Patrol (CAP), which could provide a framework that supports long-term education and retention of the US government cyber workforce.

The Problem: How to Develop a Cyber Workforce Talent Pool

The Longfellow poem of patriot Paul Revere's ride which proclaimed "One, if by land, and two, if by sea" [4] is an early acknowledgment of a warfighting domain influencing the Operating Environment (OE) that commanders considered before employing forces. The warfighting environments expanded asnew technologies provided means to strike the adversary and further national strategic objectives. The Air domain joined land and sea domains in World War I and II. Later, during the Cold War, American strategists embraced Space as a warfighting domain. Military technologies including satellite communications, electronic computers, and the Internet evolved rapidly over time and were embraced, improved, and adapted by the civilian population for widespread use to create, exchange, and store data. The civilian use of the named technologies produced what is now collectively known as "Cyberspace".

Lieutenant Colonel Karen J. Dill is an Army Signal Officer and a graduate of the Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course (JC-4ICSOC). She served in positions as a Director of Information Management, Brigade Signal Officer, Defense Coordinating Element Operations Officer, Joint Signal Planner, and is a former Assistant Chief of Staff, G6. Currently, she is an instructor at the U.S. Army Command and General Staff College in Fort Leavenworth, KS.

The term Cyberspace does not have a standard or agreed upon definition. The Tech Terms Computer Dictionary notes that the term "cyberspace" is a popular and overused term describing the virtual world of computers.[5] Various dictionaries call it "the realm of electronic communication"[6] or "the online world of computer networks and the Internet." The Department of Defense (DoD) and Department of Homeland Security (DHS) use a more expanded cyberspace definition defining it as "A global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] For this article, cyberspace refers to that definition. The Cyberspace domain is the newest military OE, and a serious concern of the President of the United States.

Nationally, the use of cyberspace catapulted United States (US) growth in both government and civilian sectors making that same cyberspace a target for exploitation. Cybersecurity is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[8] The growth of the cyber domain continued while laws and policies to shape cybersecurity practice lagged due to a lack of knowledge gap within either a centralized government or private administration. This gap increasingly opened doors for nefarious actors to exploit vulnerabilities and resulted in multiple points of hazard to national critical infrastructure and defense systems. State, non-state, and criminal actors are actively working to leverage their cyberspace capabilities to counter US national objectives

while the DoD is challenged to develop and retain an expert cyber workforce that includes a critical cybersecurity talent pool. There are existing non-cyberspace related programs from across the Armed Forces that provide frameworks for addressing the long-term development of the US cybersecurity workforce.

The Chemical, Biological, Radiological, Nuclear (CBRN) Response Enterprise (CRE) [9] and the Civil Air Patrol (CAP) are two established programs that align and professionally develop their workforce to provide a nested and multi-component approach to event response where specialized skills, knowledge, and abilities are required from private, state, and federal responders. The CRE provides an excellent model to leverage active and reserve component manpower to provide a scalable and trained response force to disasters and catastrophic events. The CRE works by delivering specialized military teams supporting a larger integrated response to a CBRN incident. The enterprise is an excellent model to investigate because as a cybersecurity response force it would provide a specialized and professional cybersecurity response at the point of need. If modeled on the CRE, a similar cyber-focused program could potentially leverage existing federal and state funding streams for training, manning, and equipping the expert teams. A lack of funding is not the only shortfall associated with a robust cybersecurity response. A significant challenge in cybersecurity is meeting continual workforce growth objectives. Apart from the CRE model, the CAP program model is a viable solution to grow and retain the overall workforce, specifically the cybersecurity workforce, which a primary concern at the highest level of government.

The White House issued the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11th, 2017 directing cybersecurity risk management of all federal networks and infrastructure* across the whole of government and to "build and maintain a modern, secure, and more resilient executive branch [Internet Technology] architecture." [10] The President directed four areas to be addressed for cybersecurity for the nation: Policy, Deterrence and Protection, International Cooperation, and Workforce Development.

The Problem: How to Develop a Cyber Workforce Talent PoolThe Proposal: Develop the Cybersecurity Workforce by Establishing a Civil Cyber Force Modeled After the Civil Air Patrol

The top priority of the DoD cyber strategy is to develop a Cyber Mission Force and a supporting cyber workforce through training, recruiting and retention, and private sector support. [11] A long-term cyberspace advantage can only be established if the US develops and retains a cybersecurity talent pool that is educated, dedicated, and integrated into society to protect the national cyberspace domain. The CAP is an established program that develops educated, dedicated, and integrated cadet and adult members. As a result of their training program, the CAP personnel are prepared to respond as part of a nested and

multi-component approach to emergency response when specialized skills, knowledge, and abilities are required from civilians, state, and federal responders. A similar Civil Cyber Force (CCF) program could leverage youth interest in the cyberspace domain, and develop the 12 to 19-year old population of innovative, future cyber professionals as part of a military or whole of nation response to a cyberspace related crisis.

The CAP, founded in 1941, is an Auxiliary of the U.S. Air Force and retains approximately 56,000 members nationwide.[12] Participants are volunteers and Total Force[13] partners who devote their "time, energy and expertise toward the well-being of their communities. The Cadet Program is developed around five program elements: Leadership, Character Development, Aerospace Education, Physical Fitness, and Activities."[14] As a result, cadets completing the program often go into military and civilian jobs where they can make a difference and excel. Similar benefits are seen in Junior Reserve Officer Training Corps (JROTC) programs that use their "education in citizenship, leadership, social and communication skills, physical fitness and wellness, geography, and civics" to produce healthy students who have integrity and personal accountability; are actively participating in the community, society, and government; and value the role of the military and other service organizations."[15] Establishing a CCF with similar program foundational elements will embed ideas including volunteerism, commitment, service, and loyalty in the future workforce. A secondary effect of a CCF program would be a stabilized force with reduced turnover of cybersecurity professionals from the workforce. This approach meets the DoD strategic pillar to improve military and civilian recruitment and retention.

CAP program membership includes cadet youth at the program's core and active adult members who serve as mentors, trainers, and program advocates. Successful CCF recruitment would mirror the CAP program with youth as the bulk of membership, supported by active adult members. Second, CAP generates community support from other groups including Friends of CAP who help fund the program, educators who support Science, Technology, Engineering, and Math (STEM) goals of CAP, and parents who encourage their cadet CAP members. CAP cadets interact with community and business leaders and have the ability to influence community opinion and support at the grassroots level. DoD Cyber Strategy notes that "Success requires close collaboration across DoD, between agencies of the U.S. Government, with the private sector, and with US allies and partners."[16] A CCF program that leverages youth, parents, educators, and community members for support, training, mentorship, and interaction will cultivate the link to the private sector. As the CCF matures and youth move on to defense, public, or private employment many will maintain social networks established through the CCF participation and service. This will achieve the second cyber strategy pillar of developing stronger private sector support.

Last, education and training is a critical requirement of the CAP for all members. Youth attend year-round programs that test them with leadership, technology, and fitness chal-

lenges. On average, cadets spend eight hours per month plus one Saturday per month conducting CAP training, and they participate in military Service, Joint, Interagency, Intergovernmental, and Multinational exercises.[17] Adult members support the program by providing mentorship and assist in promoting the cadet program. The organization as a whole maintains a curriculum of engaging STEM topics and resources that leaders and cadets use to grow their skills. CAP cadets get special tuition rates to American Sentinel University for degrees furthering the CAP mission. There are other benefits such as discounted IT products, magazines, and travel. This highlights the requirement for education that is available to all cadets.

Education is perhaps the most challenging and critical element of establishing a CCF. The National Security Agency (NSA) outreach to STEM programs employed throughout the public school system[18] and their National Centers of Academic Excellence in Cybersecurity[19] serve as a foundation for curriculum development. Likewise, the DoD's Cyber Strategic Goal for building ready forces includes support for the National Initiative for Cyberspace Education. This comprises working with interagency partners, educational institutions, and state and private sector partners to support workforce development.[20] As the CCF program matures and cyberspace capabilities change, the curriculum, goals, nd core values can be adjusted to meet future workforce requirements.

While the NSA outreach program provides a starting point, there are multiple ongoing private national cyber education initiatives built to encourage, test, and fund cyber defense skills of elementary, high school, and college students. In fact, CAP squadrons and JROTC cyber teams routinely leverage these programs and competitions as a focus for training. CyberPatriot, Hak4Kidz, and CyberCorps®: Scholarship for Service (SFS) are some of these programs.

The Air Force Association's (AFA) CyberPatriot program which began in 2009 with a national cybersecurity completion now seeks to "to inspire K-12 students toward careers in cybersecurity or other STEM disciplines critical to our nation's future.[21] CyberPatriot links industry, government, and students in a cyber defense competition between students who try to find vulnerabilities and harden the defense of a Windows system and networks.[22] The program was well received by industry professionals and is now sponsored by multiple corporations including Northrop Grumman Foundation, Cisco, Symantec, and the University of Maryland University College. The corporate interest is a proof of concept that the private sector is willing to invest in youth cyber education programs. The CyberPatriot program participation has continuously expanded and now includes AFA Cyber camps and an Elementary School Cyber Education Initiative. Their elementary cyber education initiative meets many of the requirements proposed within the CCF including encouraging students to learn about cybersecurity careers, the importance of cybersecurity, introduces cybersecurity principles, and helps students to better protect themselves.[22]

The next generation of cybersecurity workforce and experts are today's hackers. Youth-oriented "white hat" hacking events such as the traveling Hak4Kids events or the long-running Roots Asylum use hands-on workshops, games, and simulations to improve technical and STEM skills, and enable elementary and high school students to discover the joy of ethical hacking through.[24] Unlike the CyberPatriot program where teams compete to harden a network, the Hak4Kids and Roots events use problems, puzzles, and cognitive training games to exercise an individual's STEM and logic skills to stop hackers before damage is done.[25] The Roots Asylum offers a "safe playground" for kids to explore cybersecurity, cryptography, and hardware hacking.[26] These two programs grab youth interest, hone their skills in relevant technology and software, and generate an understanding of the consequences associated with hacking. Hak4Kidz and Roots Asylum both show the benefits of hands-on cyber playgrounds. CCF curriculum could include and benefit from developing and leveraging portable cybersecurity labs and cybersecurity ranges for novices to learn about old IT infrastructure which forms the national base infrastructure, as well as experiment with new and emerging technology that will enable them to defend future cyberspace more effectively and efficiently.

Last, the CyberCorps: SFS meets the financial needs of college-age students pursuing cybersecurity and information assurance career fields. The program is a National Science Foundation scholarship opportunity for students in cybersecurity-related degree programs at nation-wide select two- and four-year colleges and universities.[27] The overarching program goal is to increase and strengthen the cadre of federal information assurance professionals protecting the government's critical information infrastructure.[28] SFS is similar to the DoD's Reserve Officer Training Corps (ROTC) 2-, 3-, and 4-year scholarship program as a path to military service where cadets incur a military service obligation as military officers, so too the SFS students fulfill a federal service obligation. The tenure is based on the scholarship length. Military junior officers meet their professional obligation by serving in Active Duty, Reserve Force, and National Guard units nationwide. In the CyberCorps SFS program, graduating students receive a merit-based scholarship, and following graduation are obligated to complete a 10-week internship followed by employment in positions in federal, state, local, or tribal governments.[29] The key difference between the SFS obligation and the ROTC obligation is that the SFS students must seek their internship and post-graduation opportunities.[30] The CCF as a hybrid organization can take advantage of the CAP program youth-base and ROTC accessions structure to produce the next generation of cybersecurity professionals. The CCF would encourage and foster youth interest, loyalty, and education in a cyber curriculum like CAP; and like the CyberCorps SFS, the CCF would funnel qualified students into senior-level scholarship opportunities at approved, degree-producing, institutions with a follow-on civil or federal service obligation.

Recommendation and Conclusion

> We live in a time of growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. We are vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector. [31]

The DoD is facing an enormous cyberspace challenge, and must cultivate a cybersecurity workforce to address long-term cybersecurity requirements. There are multiple defense activities that are tested and meet specialized workforce needs. They provide an adaptable framework that supports building and aligning cybersecurity professionals to protect US cyberspace, retain the advantage, and respond to a crisis. Two essential programs, CBRN Response Enterprise and CAP, demonstrate how youth and current professionals can be leveraged to draw from involved youth to meet the workforce development and retention challenges in a multi-layered environment. A variety of government and privately sponsored educational programs and events provide a ground framework to provide state-of-the-art training while laying the groundwork for the future workforce. Further research opportunities on this topic include extensive reviewing other Armed Forces youth programs such as JROTC, U.S. Coast Guard youth programs, and scouting organizations. The DoD should investigate establishing a CCF that is modeled after the CAP, and conduct preliminary appraisals of youth cybersecurity education programs, and civil-military emergency response enterprises and programs. This is an investment that America must make to meet the threats of today and prepare for the dangers of tomorrow.

NOTES

1. Margaret Rouse, "Cyberspace," *SearchMicroservices,* accessed May 19, 2017, http://searchmicroservices.techtarget.com/definition/cyberspace.

2. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," whitehouse.gov, May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

3. Heinrich Reyes, "CBRN Response Enterprise," March 14, 2012, accessed May 18, 2017, http://dtic.mil/ndia/2012/CBRN/Reyes.pdf, 7.

Johnny Lairsey, "The CBRN Response Enterprise in the Homeland," *Small Wars Journal Blog,* August 1, 2012, accessed May 19, 2017, http://smallwarsjournal.com/blog/the-cbrn-response-enterprise-in-the-homeland.

4. Henry Wadsworth Longfellow, "Paul Revere Heritage Project," *Paul Revere's Ride,* 1869, accessed May 19, 2017. http://www.paul-revere-heritage.com/poem.html.

5. Per Christensson, "Cyberspace Definition," TechTerms, (2006), accessed August 28, 2017. https://techterms.com/definition/cyberspace.

6. "Cyberspace," *Dictionary.com.* Accessed August 28, 2017, http://www.dictionary.com/browse/cyberspace.

7. Joint Chiefs of Staff, JP 6-0, *Joint Communications System* (Washington, DC: Government Printing Office, June 2015), vii. The Department of Homeland Security definition for cyberspace is identical to the DoD joint definition.

8. Department of Homeland Security, "National Initiative for Cybersecurity Careers and Studies," *Glossary,* last modified August 2, 2017, accessed August 28, 2017, https://niccs.us-cert.gov/glossary#C. The DHS NICCS Portal's cybersecurity lexicon is intended to serve the cybersecurity communities of practice and interest for both the public and private sectors.

9. Reyes, *CBRN Response Enterprise,* 7, The CRE is U.S. Northern Command (USNORTHCOM) and National Guard Bureau multilayered organization response teams whose missions are to conduct CBRN response operations within the United States to support civil authorities in response to CBRN incidents; Johnny Lairsey, *Small Wars Journal Blog.* The CRE developed after the 1993 World Trade Center bombing under Presidential Decision Directive 39, Nunn-Lugar-Domenici Amendment 4249, National Defense Appropriations Act 2007, 2009, and 2010.

Fully established in 2012, the enterprise is a conglomeration of Title 10 units allocated to USNORTHCOM and National Guard units assigned to their respective states. The CRE consists of Weapons of Mass Destruction Civil Support Teams (WMD-CSTs), Homeland Response Forces (HRF), CBRN Enhanced Response force Packages (CERFPs), Command and Control CBRN Response Elements (C2CREs), Defense CBRN Response Force (DCRF) and Joint Task Force Civil Support.

10. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Sec 1 (c) (v).

11. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April, 2015), 17.

12. Civil Air Patrol National Headquarters, *Civil Air Patrol:* About CAP, last modified 2017, accessed May 20, 2017, http://www.gocivilairpatrol.com/about/.

13. Total Force is defined by the author as a military force including personnel from active duty, reserve component, National Guard, and auxiliary forces.

14. Civil Air Patrol National Headquarters, *Information for Parents for Prospective Cadets,* last modified 2017, accessed May 20, 2017, http://www.gocivilairpatrol.com/cap_home/parents/.

15. U.S. Army Cadet Command (ROTC), *The JROTC Program,* accessed May 20, 2017, https://www.usarmyjrotc.com/JROTC_information.html.

16. Department of Defense, "The Department of Defense Cyber Strategy" (Washington, DC: Department of Defense, April, 2015), 41, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

17. Michael Marek, "Operations Exercise Success," *Civil Air Patrol Communications Blog,* March 13, 2017, accessed on May 17, 2017, https://www.capmembers.com/emergency_services/communications-blog/?operations_exercise_success&show=entry&blogID=1827.

NOTES

18. National Security Agency, "Resources for Educators", last modified May 3, 2016, accessed on May 21, 2017, https://www.nsa.gov/resources/educators/. NSA established various outreach programs for teachers at the K-12, undergraduate and graduate levels to engage students on the importance of science, technology, engineering and math (STEM) and language education, and to inspire future generations to consider National Security and STEM careers.

19. National Security Agency, "Resources for Educators", last modified May 3, 2016, accessed on May 21, 2017, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/.

20. Department of Defense, 18.

21. Air Force Association. "CyberPatriot." *What is CyberPatriot?.* http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx, accessed November 13, 2017.

22. Air Force Association. "CyberPatriot," *History.* http://www.uscyberpatriot.org/about/history, http://www.uscyberpatriot.org/about/history, accessed November 13, 2017.

23. Air Force Association. "CyberPatriot." *What is CyberPatriot?.* http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx, accessed November 13, 2017.

24. Hak4Kids. "Hak4Kids," *About.* http://www.hak4kidz.com/about.html and r00tz Asylum, "r00tz Home" https://r00tz.org/, accessed December 20, 2017.

25. Man, Jeffrey. "Hak4kidz.com in the news," video, 1:45, April 1, 2017. https://www.youtube.com/watch?v=WSd-fVS6it80.

26. Nico Sell. "Techcrunch," *"Breaking good" by teaching kids to hack at Rootz Asylum,* August 17, 2016, https://techcrunch.com/2016/08/17/breaking-good-by-teaching-kids-to-hack-at-r00tz-asylum/, accessed December 20, 2017.

27. Department of Homeland Security, "National Initiative for Cybersecurity Careers and Studies." *CyberCorps®: Scholarship for Service (SFS)* (2017). https://niccs.us-cert.gov/formal-education/cybercorps-scholarship-service-sfs, accessed December 27, 2017.

28. U.S. Office of Personnel Management, "CyberCorps®: Scholarship for Service", *CyberCorps®: Scholarship for Service.* (2017), https://www.sfs.opm.gov/default.aspx, accessed December 27, 2017.

29. U.S. Office of Personnel Management, "CyberCorps®: Scholarship for Service", *Students: Frequently Asked Questions (FAQs) (2017),* https://www.sfs.opm.gov/StudFAQ.aspx, accessed December 27, 2017.

30. Ibid.

31. Department of Defense, 33.

Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models

Professor Frank H. Katz

ABSTRACT

In recent history, America witnessed cyber breaches at Snapchat, where employees had personal information stolen by way of a phishing scam; Premier Healthcare, which saw unencrypted data pertaining to more than 200,000 users stolen from a laptop; Verizon Enterprise Solutions, who had the information of 1.5 million customers stolen by hackers; and LinkedIn, who saw a 2012 data breach "come back to haunt them when 117 million e-mail and password combinations stolen by hackers four years ago popped up online [1]." These are just some of the many breaches experienced recently, which also included the hacking of a Presidential candidate by actors of a foreign nation-state, potentially an act of cyber warfare.

Who is going to protect US citizens from these threats? In January 2017, CSO Online reported that "A Forbes story in 2016 reported there would be 1 million cybersecurity job openings in 2017. Some things are worth repeating. There were 1 million cybersecurity job openings in 2017, give or take. Not much has changed over the past year. Can armies of interns close the cybersecurity skills gap asked a Fast Company story in September of 2016? Not likely. In the US, and internationally, there's not enough cybersecurity grads — or computer science grads with cyber credits [2]." This begs the question, "what constitutes the best practices in a cybersecurity program that will educate these future professionals?" What is the right balance between the breadth of the curriculum in such a program and its depth? This paper will attempt to answer those questions by describing how our university's NSA accredited program was created, the courses it contains, and the pedagogical methods it employs to educate and prepare future cybersecurity professionals for the workplace.

Frank Katz holds an M.S. in Management from Georgia State University (1987), and a B.A. in Computer Science from the University of Florida (1977). Upon graduating from Florida, he was commissioned a 2LT in the U.S Army, serving on active duty for four years, attaining the rank of Captain.

He has over twenty-one years of industry experience in the IT field working for companies as diverse as The Coca-Cola Company and Great Dane Trailers, Inc.

He has been an Assistant Professor at Armstrong State University, now Georgia Southern University, since 2002. While at Armstrong, he was instrumental in creating the curriculum in Cyber Security, which has been recognized as an NSA-CAE/CDE.

He has been published numerous times in Cyber Security, is an Editorial Board Member of Kennesaw State University's Journal of Cybersecurity Education, Research, and Practice, a member of ACM, and a Life Member of the Military Cyber Professionals Association.

Keywords—cybersecurity; cybersecurity education; pedagogy; curriculum; virtualization; stackable curriculum

I. HISTORY OF THE PROGRAM

When the Information Technology (IT) major was introduced at Armstrong State University (Armstrong) in 2002, there was no requirement that students take a course in either Computer or Information Security. Both Computer Science (CS) and IT students were required to take a course in Ethical Considerations in Computer Science, which has since been renamed as Introduction to Computer Ethics and Cyber Security. At the time, however, there was no course that addressed the growing field of Information Security. In recognition of this burgeoning field, in January 2006, Armstrong offered its first course in Information Security, approved as a permanent addition to Armstrong's IT curriculum. At the same time, Armstrong received funding for its Cyber Security Research Institute, a non-academic unit closely related to and funded by the U.S. Department of Homeland Security. The establishment of this research institute led the administration, the Department of Criminal Justice in the College of Arts and Sciences, and the (then) School of Computing to create an academic minor in cybersecurity to be cross-listed between Criminal Justice and Information Technology.

The curriculum would develop further, in October 2010, when the paper "Curriculum and Pedagogical Effects of the Creation of a Minor in Cyber Security" was presented at Kennesaw State University's Information Security Curriculum Development Conference (InfoSecCD), now named the Conference on CYBERSECURITY EDUCATION, RESEARCH & PRACTICE [3]. It described the issues related to the creation of an interdisciplinary minor in Cybersecurity at Armstrong, and its effect on

the university's IT major curriculum. At that time, we were not enrolling and graduating students in the minor because even though the second course in the minor had been created in the catalog, its curriculum had not been determined. Consequently, the conclusion of that paper left the fate of the minor in doubt, stating that much curriculum committee work needed to be done before the minor was either removed or properly and fully supported [3]. After attending the 2010 InfoSecCD, our department decided that the second course in cybersecurity would cover Network Security. As enrollment in the minor grew, including both IT and Criminal Justice students, we saw the need to expand our curriculum. Consequently, in the Fall of 2015, we offered our third course in cybersecurity, Ethical Hacking and Incident Response, making the minor even more robust.

II. STACKABLE CURRICULUM AS A MODEL FOR THE PROGRAM'S DEVELOPMENT

a. CACE and Potential Military Students

At this time, Armstrong created a Center for Applied Cyber Education (CACE). The Center is headed by a staff person with a military background in cybersecurity, CACE has several goals: (1) to coordinate engagement and cooperation in cybersecurity curricular efforts, such as having cybersecurity students mitigate a simulated attack, and having English/Journalism students report its findings in the student newspaper; (2) outreach to the community, as evidenced by CACE's running the Cyber Patriot program for local high school students in the Summer of 2016, and again in 2017; (3) marketing the university's cyber programs to potential civilian and military students; and (4) to engage in cyber workforce development.

Because Armstrong is located in Savannah, Georgia, near several major military installations, including the Army's Fort Stewart (3rd Infantry Division) and Hunter Army Airfield, enrolling military students was a priority. However, a challenge particular to that demographic was that military students might only be able to attend the university for just a few years before transferring to another installation. Since a student must be enrolled in a major degree program to earn a minor, this was seen as a major hurdle to overcome in enrolling military students in what was then Armstrong's sole cyber program, the minor in cybersecurity.

b. Stackable Curriculum as a Remedy

The concept of a stackable curriculum was identified as a means of resolving this challenge. Stackable curriculum, as defined in Portable, Stackable Credentials [4], allows students to earn shorter-term credentials with clear labor market value and then build on them to access more advanced jobs and higher wages. These stackable postsecondary certificates and credentials would offer an accelerated entrance to the job market; this is essential for students who need to work while in school and may not be able to wait four to six years to finally earn a marketable credential. "The majority (51%) of post-secondary

certificate programs take less than a year of instructional time to complete, while 41% take between one and two years Stackable credentials also increase the persistence and motivation of the learner by offering smaller, yet recognized subgoals [4]."

This academic concept is not new, but it was brand-new to Armstrong's Department of Computer Science and Information Technology, in which most of the courses in the minor were housed. To meet CACE's workforce development goals, we created the Undergraduate Certificate in Cyber Security, and an Associate of Science, Cyber Security Track for enrolled students not interested in earning a degree, and enrolled students majoring in various unrelated fields. We also modified the Bachelor of Information Technology (BIT) degree so to have a general IT Track and a Cyber Security Track. The premise in creating these programs was that if a student matriculated in the Certificate program, and then wanted to earn a degree, that student could earn the certificate, and then either earn the AS or BIT with the Cyber Security Track. Considered the first cybersecurity program for student enrollment, the certificate was created to only require six courses in IT and cybersecurity, with only one prerequisite – college algebra.

In the Spring semester of 2015, Armstrong began its year-long attempt to earn the coveted NSA-CAE in CDE designation. Armed with a curriculum that included four courses solely dedicated to Cyber Security and the Interdisciplinary Minor in Cyber Security program, this was a rigorous and time-consuming effort. Although the curriculum presented to the NSA-CAE reviewers was the Minor program that included cybersecurity, Armstrong included the nascent Undergraduate Certificate and AS in our application. Armstrong was awarded its designation in December 2015 and presented with the designation certificate at the National Cyber Summit in June 2016.

III. COURSES IN THE PROGRAM – BREADTH VS. DEPTH

In any educational setting, one of the great debates is whether a program of study provides both breadth and depth of knowledge in that curriculum. When teaching information security, one way of defining breadth is "where we want to ensure that our students understand fundamentals of the various components that are at play in information security [5]." This includes computing but also includes other disciplines, such as law, psychology, ethics, and communication skills. "Depth in this area is where we sacrifice some of that breadth for additional skills, training, and practice in some of the specific tools, skills, and knowledge directly related to the practice of a particular area of information security [5]."

a. Breadth of Education in Armstrong's Cybersecurity Programs

In "The Case for Depth in Cybersecurity Education", the authors state that "all CAE/IAE (Information Assurance Education, now CDE, or Cyber Defense Education) schools must map their curriculum to government information assurance standards. While these

standards provide a broad approach to teaching cybersecurity, employers increasingly desire depth and breadth of knowledge[6]." This implies that the NSA-CAE program's standards do not promote depth of knowledge in cybersecurity. Having gone through the process of becoming a CAE institution, this is not necessarily accurate. Armstrong's cybersecurity curriculum has breadth by taking a holistic approach in teaching cybersecurity, holistic in that learning cybersecurity is not just learning technology. Our curriculum integrates the "pillars of people, process, and technology[7]", as all three are crucial for implementing cybersecurity solutions. We accomplish this in many of our IT and cybersecurity courses through not just labs, but case studies, exercises, and role-playing scenarios involving non-technical aspects of the discipline. We teach various components of cybersecurity starting with the fundamentals of Computer Science, touching on it in courses on Operating Systems, Data Communications, Systems Analysis and Design, and Network Design and Administration. There is hardly a course in our IT curriculum, exclusive of our cybersecurity courses, which has not been mapped to the NSA-CAE Knowledge Units (KUs).

b. Depth of Education in Armstrong's Cybersecurity Programs

The depth of instruction in the curriculum is just as important. The article describes depth in cybersecurity education as starting in high school education, including competitive initiatives such as the Cyber Patriot program. These College competitions also lead to depth in education. However, depth can also be "supported and even inspired in a classroom; however, students must take what they learn and apply it independently. Classroom experiences that support depth must focus on the learner as opposed to the instructor; they must offer continuous assessment with rapid feedback and the ability for the learner to focus and direct their learning to meet current tasks[6]." Manson and Pike's research highlights "A 2009 Washington Post article covering the debate between depth vs. breadth in science education defined depth as focusing on a few topics so students have time to absorb and comprehend the subject vs. breadth as covering every topic so students can get a sense of the whole and can later pursue those parts they find interesting[6]."

Since the depth of cybersecurity education is so important, how do we support that principle in our curriculum? We do this in two ways: (1) by our courses, and (2) by the methods used to teach the courses. Our students begin their study of cybersecurity through two general courses: CSCI 2070, Introduction to Computer Ethics and Cyber Security, and ITEC 3700, Cybersecurity I, Fundamentals of Information Systems Security. However, the remaining courses in our curriculum support the principle of depth in education by focusing on just three topics: network security, ethical hacking, and cyber forensics. ITEC 4200, Network Security, focuses solely on endpoint security—the use of firewalls and VPNs to secure a network. ITEC 4300, Ethical Hacking, emphasizes the ability of a student to penetrate a network and conduct reconnaissance, hack it, and then learn how to defend

such a network. CRJU 5003U, Cyber Forensics, is taught by the Criminal Justice department. This course is part of our minor, and it emphasizes real-world labs which allow the students to use various laboratory tools to examine digital media looking for potentially incriminating evidence. In the Spring 2017 semester, we also introduced a special topics course in Cyber Warfare, taught by the Director of CACE. This course was such a success that it might be made a permanent course in our curriculum, although short of offering a major in cybersecurity, degree requirements in the current BIT cybersecurity track may force it to be offered in our undergraduate minor or certificate.

The second way we support the principle of depth is through our instructional methods. Benjamin Franklin said: "Tell me and I forget, teach me and I may remember, involve me and I learn [8]." In keeping with that principle, it is vitally important to include hands-on laboratory work in a valid cybersecurity curriculum. "Instructors may want to be imaginative and create their own case studies and laboratory exercises, but time, and especially in the current era, financial constraints, affect all faculty members [9]." Rather than build our own labs, we have chosen to use virtual online labs, originally provided by the publisher of our textbooks, Jones and Bartlett Learning, and more recently, by InfoSec Learning. Regardless of provider, the advantages of using virtual labs far outweigh the time, cost, and physical plant required to create our own labs. In addition, virtual labs, run in the cloud, enable our students to perform the labs and associated exercises from anywhere, especially at home. However, the best way that these labs encourage learning in depth is that they focus on the student rather than the professor. The student must navigate a prescribed set of exercises, and will either receive positive or negative feedback from the labs based on their success in performing the exercises. Both providers include lab quizzes and challenge exercises, which provide immediate feedback to the students. Also, not only do many of the labs progressively build on material learned from previous labs, but they are directly correlated, on a chapter by chapter basis, to the material taught in the classroom and the textbook.

c. Depth of Education—Repetitive Skill Development

Repetitive skill development is an important way of measuring the depth of a curriculum [6]. "In his book Outliers, Malcolm Gladwell describes the 10,000-Hour Rule as a key to success in any field through practicing a specific task that can be accomplished with 20 hours a week for ten years. Ongoing changes in technology and national security needs require aspiring excellent cybersecurity professionals to set a goal of 10,000 hours of relevant, hands-on skill development [6]." While it is not possible for our curriculum to provide 10,000 hours of hands-on work in cybersecurity, our labs do provide a measure of repetitive skill development. For each course, several of the labs use the same virtual machines and tool to perform different functions and analysis. In this way, the students become more familiar with the tools. For example, throughout the labs used in the Network

Security course, the students repeatedly use: a Windows Server attack machine; a Kali Linux attack machine; Nmap; Zenmap; Wireshark; netstat; ping; port forwarding and NAT; various different common protocols including FTP, SSH, HTTP, SMTP; and various different firewalls, including native Windows Firewall, the Linux-based Endian firewall, and the pfSense firewall; learning how to configure and use RADIUS for access control; and learning how to configure and use various VPNs, including the PPTP and OpenVPN tools. The repetitive use of these tools in different exercises provides an effective means of teaching cybersecurity to our students. In a survey of Network Security students taken at the end of the Spring 2017 semester, out of nineteen students: 78,9% agreed or strongly agreed that they "understood the learning outcomes of the InfoSec Learning labs; 89.5% agreed or strongly agreed that the "lab questions and required screenshots in the InfoSec Learning labs reinforced and supported the learning outcomes"; and 94.7% agreed or strongly agreed that they "learned the lab concepts from the InfoSec Learning labs."

d. Depth of Education – Scalability

Another benefit of using online virtual labs is their scalability. On January 5, 2017, it was announced that as of January 1, 2018, Armstrong would consolidate with Georgia Southern University, in Statesboro, Georgia. On that date, we changed from a university of approximately 7,000 students into one with about 29,000 students, the fourth largest university in Georgia. Georgia Southern does not have any undergraduate programs in cybersecurity, and will essentially be acquiring ours. As students currently enrolled at Georgia Southern discover the new cybersecurity programs, we expect their enrollment to increase. This may require an increase in online delivery of our cybersecurity courses. The need to scale up lab exercises to support our curriculum will be significantly enhanced by using virtual, online labs.

IV. CONCLUSION

Developing and implementing an effective cybersecurity education program must incorporate both breadth and depth of educational practices. An effective cybersecurity program in an organization or corporation does not exist in a silo. Similarly, breadth of knowledge is vital to a useful university cybersecurity program of study because a student must understand the totality of the field and how it interacts with many other disciplines. However, the depth of education in cybersecurity is just as important, if not more important, because it ensures that students receive instruction and skill development in specific topics needed to become entry-level practitioners in the field. Our program at Armstrong is well on its way to providing such a solid education, and will only grow as we consolidate with Georgia Southern University in 2018.

NOTES

1. Retrieved from J. Leary, (December 16, 2016), The Biggest Data Breaches in 2016, retrieved June 26, 2017, from https://www.identityforce.com/blog/2016-data-breaches.

2. Retrieved from S. Morgan, (January 8, 2017), One-million cybersecurity job openings in 2017, retrieved June 26, 2017, from http://www.csoonline.com/article/3155324/it-careers/1-million-cybersecurity-job-openings-in-2017.html?upd=1498495039447.

3. F.H. Katz, "Curriculum and Pedagogical Effects of the Creation of a Minor in Cyber Security," presented at the 2010 Information Security Curriculum Development Conference (InfoSecCD 2010), October 1-2, 2010, Kennesaw State University, Kennesaw, GA. Published in the proceedings of the conference and in the Digital Library of the ACM.

4. J.T. Austin, G.O. Mellow, M. Rosin, and M. Seltzer, "Portable, Stackable Credentials, A New Education Model for Industry-Specific Career Pathways," McGraw-Hill Research Foundation, 7, November 2012.

5. D. Burley, "Interview With Gene Spafford on Balancing Breadth and Depth in Cybersecurity Education," in ACM Inroads, March 2014, 42-43.

6. D. Manson and R. Pike, "The Case for Depth in Cybersecurity Education," in ACM Inroads, March 2014, 47-51.

7. J. LeClair, S. Abraham, and L. Shih, "An Interdisciplinary Approach to Educating an Effective Cybersecurity Workforce," presented at the 2013 Information Security Curriculum Development Conference (InfoSecCD 2013), October 12, 2013, Kennesaw State University, Kennesaw, GA. Published in the Digital Library of the ACM.

8. Retrieved on June 27, 2017 from http://www.goodreads.com/quotes/21262-tell-me-and-i-forget-teach-me-and-i-may.

9. F.H. Katz, "Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance," presented at the 2013 Information Security Curriculum Development Conference (InfoSecCD 2013), October 12, 2013, Kennesaw State University, Kennesaw, GA. Published in the proceedings of the conference and in the Digital Library of the ACM.

Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law

Dr. Catherine Lotrionte

INTRODUCTION

In 2012, then-Secretary of Defense Leon Panetta spoke about the rising dangers of a "cyber Pearl Harbor," analogizing the potential devastation from a cyberattack to that of the surprise attack on the U.S. naval base in Hawaii in December of 1941.[1] More recently, U.S. Senator John McCain called the Russian meddling in the 2016 elections "an act of war."[2] The reality of contemporary international relations and the proliferation of cyber operations as an adjunct to both peacetime and wartime operations of states has raised important questions about what would constitute an act of war in the cyber domain, triggering the relevant international legal rules regulating state behavior. As of yet, there is no global consensus about what an act of war carried out by cyber means would look like, versus acts that would fall below the level of an act of war, and although still unlawful, would call for different responses under the law.[3]

State actions short of war have been around for a long time. But the current ambiguities in the law related to cyber operations, where details of the international legal principles and rules are poorly defined and subject to competing interpretation or contested application, have left policymakers uncertain about the applicable legal framework for certain actions, and hesitant to respond to those states exploiting the ambiguities as they violate the law with impunity. Furthermore, this lack of clarity in the law creates the potential to misread the intentions of other states that could unnecessarily lead to escalation.

With this in mind, at the outset of this article it is necessary to differentiate between (a) "war" as a figure of speech used for its rhetorical power for political purposes, to heighten the effect of an argument or a news story in the media and (b) "war" as a legal term of art that has special meaning for state conduct under international law.

Dr. Catherine Lotrionte is a Brent Scowcroft scholar at the Atlantic Council with the Cyber Statecraft Initiative in the Scowcroft Center for Strategy and Security, and the Founder and former Director of the CyberProject at Georgetown University where she has taught international law and national security law.

Dr. Lotrionte has served as Counsel to the President's Foreign Intelligence Advisory Board at the White House and as Assistant General Counsel at the Central Intelligence Agency. She has a JD from New York University Law School, MA, and Ph.D. from Georgetown University.

While it is accepted that the need to define war is still relevant for some branches of domestic law; for example, in the context of "war powers" in constitutional law and that it is a political question, solely for the determination of those political departments of a government of a state, as to whether a country is or is not engaged in war at any specific time, in so far as contemporary international law is concerned, the definition of war has little bearing on legal analysis. Although there is no one binding definition of war, elements that are common to all proffered definitions under international law, and accepted for purposes of this article, is that war is "a contest between states" [4] involving a "comprehensive" use of force. [5] In other words, war exists when peace between states has ended, and a certain quantum of hostilities has commenced. While both states and non-state actors implicate the rules related to conflict covered in this article, due to space limitations, this article focuses on state activities and only those actions by non-state actors that are attributable to states.

Rapid technological advances and the changing character of conflict, where threats are less easily defined, attackers can more easily deny responsibility, and the existing ambiguities in the rules are readily exploited by aggressors, has posed new challenges for states in defending their national interests. Today revisionist states actively seek to topple the post-WWII international order, including the rules it is based on, using coercive measures falling below the legal thresholds that traditionally allow for forcible responses. [6] By taking advantage of ambiguities in the law they can sow doubt in the lawfulness of responses, eliminating, limiting or delaying responses. In this manner, they are skirting the laws and shifting the international rules, as they try to rewrite them, in their favor. As

evidenced by state practice and government officials' statements,[7] these states purposely operate in a gray zone area of conflict, falling between the normal peacetime relations between states, and the state of full-blown overt war or armed conflict.[8] For sure, even outside the cyber context, ambiguities and differences about the rules related to use of force have long existed among states. Such gray zone operations, short of armed conflict, have historically manifested in all domains, but in cyberspace adversaries have unparalleled advantages compared to other domains because the rules are even less developed and state practice is still evolving.[9] In this respect, the existence of complicated questions about cyber operations related to the international law concerning the use of force is not in itself a new development, it is just about applying some old questions about the law to the newest development in technologies used by states.

Given the different legal consequences that apply depending on whether a state is involved in a war or not, it is important to distinguish between war in the formal legal sense and other kinds of conflicts that fall short of war involving the use of force such as defensive action, reprisal or countermeasure, intervention, or forcible measures not constituting uses of force. The vast majority of hostile cyber operations carried out by states to date fall into the category of actions short of war and, therefore, this article focuses on the challenges of determining what actions by states in cyberspace short of war are prohibited in international law. Certainly, not every hostile act in cyberspace creates a state of armed conflict between nations, but the important question that this article addresses is when, and in what manner, a state can take action through cyberspace or otherwise, in response to hostile cyber operations short of war that threaten the security of the state.

In the context of cyber operations, in recent years governments have affirmed the general applicability of existing international law to states' activity in cyberspace in both peacetime and wartime, recognizing that although there is no global treaty regulating cyber operations, existing treaties, customary rules and general principles of international law[10] can be extended to cyber operations through the interpretation of existing sources of law.[11] Although existing international laws such as the United Nations Charter (Charter) and the law of armed conflict cannot claim to be directly applicable to cyber operations, given that cyber operations were not even contemplated by those state officials drafting the laws at the time, states have looked to the "spirit" of the existing laws to adapt them to the current threats and new technologies, acknowledging that international law, like the Charter, is a "living, growing" system of rules that are capable of adapting to the needs of the international community through the process of the evolution of customary practice and *opinio juris.*[12] These principles are fundamental to the rule of law in cyberspace no less than any other domain.

Today, while there remains little disagreement over whether international law ought to be applied to cyber operations conducted by states, there is much contention over the

precise application and content of many of the specific rules.[13] Efforts to clarify and reach agreement on international rules for cyberspace have been ongoing, both inside national governments, in international bodies,[14] and through the work of legal scholars,[15] but the recent failure in 2017 of the 25 members of the 2016-2017 UN-sponsored Group of Governmental Experts (UN GGE) to reach consensus on the precise manner which the rules apply is a troubling development, and an indication that legal ambiguity persists.[16]

As states have yet to clearly define the contours of the law in this space, legal scholars have played an important role in trying to distill some common understanding of the applicable law. In particular, the work of the Group of International Experts who authored the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (Tallinn Manual 2.0)*[17] has usefully contributed to efforts to bring clarity to what the law says about cyber operations and to highlight where the law remains unsettled in this area. Even among the group of experts, there were many issues on which the group failed to achieve consensus, as is reflected in the commentaries of the rules. Although the *Tallinn Manual 2.0* is a non-binding document, such scholarly work has bolstered government efforts to develop the law in this space. In lieu of an international treaty for cyberspace, unlikely to be negotiated in the near future, if ever, it will be for the states to develop the law through the complex, and not always transparent, process of custom. This process will take time as state practice in cyberspace is still at an early stage, not always publicly visible, and state *opinio juris* is limited. This situation raises the importance of efforts by government officials and non-governmental entities to bring more clarity to the international rules that govern aggressive state actions short of "armed attacks."

This article examines how cyber operations fit within the modern system of international laws related to the use of force, and where circumstances require, how the rules may be adapted and modified to accommodate this new method of conflict, helping to answer the questions: What hostile state activities, short of war, are prohibited in cyberspace, and what measures can states take in response to such hostile cyber operations?

MODERN INTERNATIONAL RULES FOR WAR & PEACE

At the start of the 20TH century, with the development of more technologically advanced and more lethal weapons, states saw the value of binding agreements limiting the right to resort to armed force. The new rules promoting peace codified in The Hague Conventions of 1899 and 1907,[18] however, had little impact in restraining states' resort to war in 1914. Nor did the Covenant of the League of Nations, adopted in 1919,[19] placing restrictions on the resort to war or the 1928 Kellogg-Briand Pact,[20] outlawing war as an instrument of national policy, prevent Japanese aggression against China in 1937, the 1935 Italian aggression against Ethiopia, and Nazi aggression that triggered the most destructive war in history.

As states adopted the Geneva Conventions of 1949, a new concept of "armed conflict" was introduced, establishing that the application of humanitarian laws was no longer dependent on the will of states to make formal declarations of war but rather the facts on the ground would determine whether a situation was one of war or peace. Previously, states avoided being bound by the "rules of war" by denying the existence of a state of war. Today, it is a settled norm of international law that a formal declaration of war is not a necessary condition for a state of armed conflict to exist.[21] As the legal meaning of "war" lost its relevance, the determination as to when the rules related to conduct in hostilities were triggered would, going forward, be based on an assessment of the intensity and protracted nature of the fighting and the nature of the groups.

According to conclusions of the International Law Association's Committee on the Use of Force, in their study on the definition of war in international law, an armed conflict exists when there is an intense exchange of fighting by organized armed groups.[22] In line with a "first-shot theory," as soon as the first person is affected by the conflict or the first attack launched, the humanitarian laws of the Geneva Conventions apply.[23] Based on this approach, it does not matter where the initial violent act takes place, on the high seas, in outer space or cyberspace, or how the violent act is carried out, air raids, shelling or cyberattacks, its duration or number of casualties, any use of arms by states and organized groups above a *de minimis* threshold will activate an armed conflict and trigger humanitarian laws. Once a state of armed conflict exists, all rules related to how the hostilities should be conducted apply. This fact-based approach to determine when a state of war begins has been widely accepted within international law. Similarly, a proper assessment of when an armed conflict has commenced in cyberspace will depend on the facts of the particular circumstances, and whether the requisite level of hostilities has commenced.[24] There has been a general consensus among states that cyber operations carried out during hostilities, as long as those hostilities meet the threshold for armed conflict, will also be covered by the rules of international humanitarian law.[25]

The UN Charter Framework

By the 20TH century, international law was undergoing a metamorphosis, a revolution concerning inter-state conflict. As the rules concerning the manner in which states would fight their wars were being codified, and new rules negotiated, other rules were established concerning the initiation of armed force during peacetime. The new rules emerged first in the 1928 Kellogg-Briand Pact for Renunciation of War as an Instrument of National Policy in a somewhat restrained fashion, and then, in a sweeping prohibition of the threat or use of force in international relations, in article 2(4) of the Charter.[26] In contrast to classical international law in the 19TH and early 20TH century, when states had the right to resort to war or initiate hostilities and reprisals to enforce their rights, address an injustice and collect debts owed, and the use of force was the common means to obtain redress and

ensure law enforcement in the international legal order, by 1945, with the drafting of the Charter, the prohibition of the use of force underwent considerable development with a ban on forcible coercion under article 2(4) that clearly outlawed physical coercion, even for the enforcement of legal rights. As proclaimed by the International Court of Justice (ICJ), in 1986, this prohibition on the use of force was reflected in customary international law [27] and today is acknowledged, in some respects, as a peremptory rule or rule of *jus cogens,* with widespread acceptance of its applicability to cyber operations conducted by states. [28]

Article 2(4) Use of Force Threshold: What's Covered and What's Not

The Charter's article encompassing the ban on the threat or use of force was drafted in response to the failed attempts of the international community to outlaw and prevent wars. With the intent "to save succeeding generations from the scourge of war," [29] the state officials who drafted the Charter sought to incorporate not only direct armed attacks by states that would lead to war, but also other forms of force below an armed attack threshold as well. The drafters, therefore, avoided the use of the terms "war" or "acts of war" within the article, making the terms obsolete for purposes of the modern international laws related to *jus ad bellum.* On the one hand, the article 2(4) prohibition was intended to "state in the broadest terms an absolute all-inclusive prohibition" on the aggressive use of force between states, prohibiting armed force or the equivalent of armed force. [30] On the other hand, there would be minimal uses of armed force that would fall outside of article 2(4), not meant to be covered by the provision.

The article proclaims:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. [31]

Since its adoption, the article's scope has been clarified through state practice, and *opinio juris,* and ICJ interpretation. In the first instance, the type of force prohibited in article 2(4) is armed force, or the equivalent of armed force, causing violence, as compared to other types of coercive conduct that would not directly cause such violence [32] For instance, non-armed force that could include forcible or coercive measures such as economic sanctions, diplomatic protests, psychological operations, and the unconsented presence of official ships and submarines within a state's territory is excluded from the scope of the article. [33] These forms of coercion are covered by the principle of intervention in the internal affairs of other states and are not forbidden *per se* but only when they become excessive, targeting an area in which the state has sole discretion to decide freely.

Even within the category of armed force, article 2(4) does not cover all armed force. Armed force of a minimal or *de minimis* amount of force will not be covered under the

article if the acting state has no intention of challenging the state in which it using the minimal force. The role of intent in assessing whether an action is a use of force finds support in ICJ case law as well as state practice.[34] The intention in question is not one of motivation for the acts but rather the intention to be considered is that of forcing the will of another state. The intention cannot make an act that violates a rule become consistent with the rule, for example, in the case of arguments in support of interventions for humanitarian purposes. But it can, before any legal determination, affect the determination of the relevant field of law for consideration, for instance, the use of force regime under the Charter versus another legal regime such as international criminal law, international communications law, law of the sea, etc.

Although article 2(4) may not cover minimal forcible actions with confined intent and purposes, depending on the circumstances, such actions may be regulated by other principles of international law such as non-intervention or other treaty-based legal regimes.[35] In assessing the applicability of article 2(4) in various circumstances, the gravity of the force is relevant as well as the intent of the state to use force against another state.[36] If the force used is not excessive and the state acting does not intend to use force against the state, the actions may not be covered by the prohibition in article 2(4). For example, if a state through cyber means interrupts the operations of a command and control server within another country without its consent in order to stop cyber intrusions against the acting state's banks for instance, because the force was minimal and not intended to force the will of the other state, it may be considered not to constitute the type of force that article 2(4) was meant to cover. Likely to be excluded from the scope of article 2(4) would be the disruption of Internet service by denial of service attacks. These cyber actions will not as a general matter fall within article 2(4). If these actions are characterized as unlawful, it would likely be so not in respect to article 2(4) but more generally of the principle of state sovereignty, the norm of non-intervention or other bodies of law relevant to the context of the situation.

States have agreed that cyber operations can violate article 2(4) of the Charter, the principle of non-intervention under customary international law and other *lex specialis* rules, however, there remains a debate as to whether cyber operations that do not violate these laws may still violate the customary legal principle of sovereignty in carrying out cyber operations within the territory of another state without its consent. Although a review of this issue is beyond the scope of this article, it is worthy of brief mention to highlight what seems to be an area of disagreement and unsettled law. The basic legal question is what types of actions would be covered by the principle of sovereignty under international law as applicable to cyber operations. There are conflicting views among scholars on this issue[37] with government officials recently weighing in on this debate, providing some valuable insight into how the law may be developing on this issue. In May 2018, the United Kingdom (UK) Attorney General, speaking for the first time in such detail, set out the UK's

legal position on some specific international rules for cyber operations, to include the principle of sovereignty, and highlighting areas of disagreement with previous interpretations of the rules for state responsibility. Related to the issue of sovereignty, the Attorney General rejected any cyber-specific rule related to the "violation of territorial sovereignty" from cyber operations that cause "interference in the computer networks of another state without its consent" that fall below the threshold for a violation of the rule of non-intervention. [38]

Taken together with prior statements by US government officials, generally in line with the UK statement although less detailed, these statements would indicate that some states are interpreting the rule of sovereignty as one that would not necessarily cover cyber operations causing minimal impact on another state's infrastructure as long as they do not trigger the prohibition on the use of force, the norm of non-intervention or any other existing treaty obligation. Under this approach, examples of cyber operations not implicating the sovereignty rule could include implanting of malware on another state's infrastructure and interruption of Internet service through a denial of service attack, among other possibilities. Given the historical practice of states acceptance, albeit in a seemingly reluctant manner at times, of activities of foreign governments within their territory without their consent, the UK approach seems to make the most sense. After all, it has not been the case in state practice that mere minor intrusions into territorial property with limited impact on the state would constitute an internationally wrongful act. Had this been so, the reality of the day-to-day activities of intelligence agencies would be dramatically different.

The apparent acceptance, at least by the UK, of a minimal effects test for the rule of sovereignty in cyberspace is in line with a minimal effects or gravity test for uses of force as outlined in this article, and may be most relevant to cyber operations that persist at a low level of intensity. This approach for assessing what constitutes a use of force, although of debate by some legal analysts, is gaining acceptance with support found both in state practice and the implications of ICJ decisions where not all forcible measures that contain a foreign element have been found to constitute a prohibition of article 2(4). [39] In such instances the focus has been on the assessment of the gravity of the action and the intention of the actor, or purpose of the action. [40] In one of its earliest cases, the *Corfu Channel*, the ICJ indicated that minimal uses of force not used "for the purpose of exercising political pressure" on another state would not constitute a use of force under article 2(4). [41] Although the Court ruled that the UK's minesweeping operations in Albania's territorial sea violated its sovereignty and used the phrase, a "manifestation of a policy of force" in describing the British actions, the Court did not conclude that such action violated article 2(4). [42] In a number of other situations, in enforcement cases involving maritime enforcement, law enforcement actions involving the arrest of someone in another state's territory without authorization, environmental protection acts, hostage rescue operations, and the interception of foreign aircraft that has entered a state's airspace without permission, the minimal armed

force that was used was found not to be covered by the regime on the use of force under article 2(4) but rather by other areas of international law. [43] State practice has confirmed that such actions convened as enforcement measures by states, limited in scope and intensity, with no intention to use force against the other state, do not come under article 2(4) but rather other specific rules relevant to the case at issue. [44]

A central question for cyber operations, and the primary focus of this article, of whether a hostile cyber operation by a state is an article 2(4) use of force violation, an unlawful intervention or an armed attack, is critical to the determination of what responses would be legal under international law. Even though the intent of the framers seemed clear in drafting article 2(4) that certain coercive measures would not be covered, and the long practice of states under the Charter has demonstrated support for that intent, without a precise definition of the term "use of force" within the treaty, practitioners and scholars continue to disagree over the meaning of the term "use of force." They have struggled to establish a single approach for distinguishing those actions by states that would fall within the article 2(4) regime versus those that would fall under different legal regimes, and for those actions that do fall under the regime of the use of force, which actions would fall below the article 2(4) threshold and which ones would surpass the threshold. [45] In the context of cyber operations, there remains much contention over the specific cyber operations that would violate article 2(4), fall outside the scope of the article, fall below the threshold of the article, or surpass the threshold and reach the level of an armed attack. What is of general agreement in the context of cyber operations is that for such operations to constitute a use of force under international law they must be attributable to a state, reach the gravity threshold for the use of force as meant by article 2(4), and must be exercised in the context of "international relations" between states. [46] For those cyber operations that meet these requirements and are regulated by the Charter regime, they constitute a use of force, and therefore there must exist a "proper legal basis" for them in order not to violate the prohibition within article 2(4). [47]

Historically, in trying to delineate clear lines of distinction under the law between state actions that would constitute uses of force versus other actions, international legal scholars disagreed over the appropriate focus for assessing the legality of such actions. The different proposals involved focusing on the instruments or weapons used, the characteristics of the targets, the intent of the attackers or the effects generated by the actions. [48] Ultimately, the dominant approach that has been accepted, for cyber operations as well, is one based on the effects of the actions. [49] In line with an effects-based approach, kinetic operations that have a direct destructive impact on property or injurious effects on persons, beyond a *de minimis* effect and under circumstances where the regime of use of force is applicable, would constitute armed "uses of force" and, therefore, illegal under article 2(4). Analogously, under an equivalence approach for cyber operations, states have

assessed that cyber operations that cause or are reasonably likely to cause similar damaging consequences or effects as those produced by kinetic weapons, with physical damage to persons or property, excluding those actions of *de minimis* effects not covered by the article 2(4) use of force regime, would be a use of armed force action prohibited by article 2(4). [50]

While it is virtually uncontested that cyber operations, which cause or are reasonably likely to cause physical damage, loss of life or injury to persons would fall under the prohibition contained in article 2(4) under this equivalence test, the question remains how to characterize cyber operations that produce damaging consequences but no physical destruction. In other words, is there a minimum threshold of gravity that the consequences of a cyber operation must reach to be a violation of article 2(4) versus, for example, the norm of non-intervention? [51]

For those cyber operations that are disruptive, interrupting the functionality of a target, but failing to cause lasting physical damage, a strict effects-based equivalence test under the law raises questions as to whether such attacks would constitute a "use of force" under article 2(4). [52] Such a narrow approach based on kinetic effects fails to take into account the dependency of modern society on the functioning of computer networks. It is now possible for critical infrastructure to be compromised, and society crippled without destroying the computer networks themselves. Government officials have raised concerns about the devastation that would occur if such critical infrastructure were disabled by a cyberattack, causing cascading effects between sectors and second and third-order effects disrupting societal, economic, and governmental functions. [53] The question remains then today, for cyber operations against those physical or virtual systems and assets of a state, the disruption of which would render them ineffective or unusable causing devastation to a state's security, economy, public health and safety, and environment, would they constitute uses of force in violation of article 2(4) or even an armed attack?

There exists little doubt that as a practical matter a state targeted by a cyber operation that shuts down its electric grid, leaving millions without power, disrupting the financial markets and government communications, though without causing immediate physical damage, would be considered a "use of force," if not an "armed attack." [54] And yet, under an effects-based equivalence approach, such attacks would not constitute uses of force against the state without some level of physical damage. [55] On the other hand, a more flexible interpretation of article 2(4), one based on the intent and logic of the Charter provision, the ruling in the *Nicaragua* case, [56] and a broader meaning of a "use of force" for cyber operations specifically targeting critical infrastructure may be gaining support from international legal experts and governments. [57] Such an approach would more effectively address the potential for devastating effects from cyberattacks against critical infrastructure and could encompass cases of cyber operations that significantly disrupted,

for extended periods of time, the functionality of critical infrastructure causing significant negative consequences, albeit no physical damage, to the national security and welfare of the state and citizens. The requisite level of disruption would have to go beyond mere inconvenience and "significantly disrupt the functioning of critical infrastructure," versus solely non-critical infrastructure, to fall within the scope of article 2(4). [58] This approach, in line with the decision in *Nicaragua*, although not providing the injured state with a right of self-defense, does provide it with recourse to other measures under international law that will be discussed later in this article. [59]

Below Article 2(4) Use of Force Threshold: Getting to the Gravity Question

The Charter framers recognized that aside from using armed force, states also employed other non-forcible but coercive measures in their international relations with other states to influence them. The *travaux preparatoires* of the Charter reveal that the drafters made a conscious decision not to include these other non-armed, non-violent coercive measures within the Charter prohibition on the use of force in article 2(4). [60] Coercive non-armed measures, such as economic or psychological coercion and political pressures, were purposely left outside the Charter framework. [61] Rather, these activities would either be covered under a customary international legal principle such as non-intervention [62] or be left unregulated by the law. As distinguished from uses of force that violate article 2(4), violations of a state's territorial integrity and the principle of non-intervention can occur "with or without armed force." [63] In short, the type of force prohibited by article 2(4) is armed force or the equivalent of armed force, in contrast to other types of forceful coercive conduct.

In addition to the non-armed coercive measures that fall outside of article 2(4), like economic sanctions, there are additional measures that might be "armed" or involving some minimum form of physical force, but would fail to constitute a use of force for purposes of article 2(4) because they do not meet a minimum threshold of gravity. [64] In other words, they are minimal uses of armed force that article 2(4) was not meant to cover. This methodology of using a gravity test to distinguish different levels of force for assessing article 2(4) violations is based on the same methodology used in the *Nicaragua* case to distinguish article 2(4) uses of force from armed attacks under article 51, analyzing the scope, intensity, and duration of the action. The reasoning behind using this same methodology to determine the article 2(4) threshold for uses of force and distinguishing article 2(4) uses of force from other actions, although possibility illegal, falling outside of article 2(4) is threefold: firstly, such minor uses of force that serve limited intentions and purposes are not equivalent to the purposes of those uses of force as intended to be outlawed by article 2(4), secondly, these minor uses of force do not implicate the "international relations" between states that article 2(4) explicitly incorporated into its language, and thirdly, these uses of force have a lesser level of intensity that falls below the threshold of a use of force that was intended by article 2(4) of the Charter. [65]

This approach for uses of force "appears to be gaining ground in legal doctrine" [66] based on state practice, the implications from ICJ decisions, and commentary by scholars and state officials. [67] According to the Independent International Fact-Finding Mission on the Conflict in Georgia, the "prohibition of the use of force covers all physical force which surpasses a minimum threshold of intensity" and "[o]nly very small incidents lie below this threshold, for instance, the targeted killing of single individuals, forcible abductions of individual persons, or the interception of a single aircraft." [68] In the cases of actions such as police or security operations where the force used is of a low intensity, not intended to force the state to do or not do something against its will, not engaging the relations between states, they have been characterized as falling outside the coverage of article 2(4). Such operations have included: individual international abductions, extraterritorial criminal enforcement measures, "hot pursuit" against criminals on land, enforcement actions at sea, neutralization or interception of aircraft entering a state's airspace without authorization, rescuing nationals abroad, small-scale counterterrorism operations abroad, to the targeted assassinations carried out by secret services in another state, "where the coercive character of the operation within the foreign territory is very limited" and is not targeted against the state. [69]

Outside of the cyber context, the recent case of Russia's poisoning of a former Russian spy in the UK provides insight into how states categorize various actions under the law, in accordance with the minimal threshold approach to uses of force. In her initial statement to Parliament on the matter, British Prime Minister Theresa May forewarned that unless Russia responded to the UK's accusations that Russia had used a military-grade nerve agent to kill someone on British soil, May stated, "we will conclude that the action amounts to an unlawful use of force by the Russian State against the United Kingdom." [70] In her statement, the Prime Minister never invoked the Charter or article 2(4) explicitly, although referring to an "unlawful use of force." Notably, however, in the joint statement on the matter released by the UK, the US, Germany, and France, a few days after May's initial statement, the four countries described Russia's action as "an assault on UK sovereignty and any such use by a state party is a clear violation of the chemical weapons convention and a breach of international law." [71] In that statement, there was no mention of a use of force or article 2(4) of the Charter. Rather than assessing Russia's actions under the use of force regime, the UK, US, Germany, and France treated the poisoning of a foreigner on UK soil as a violation of the United Kingdom's sovereignty and a breach of the rules related to the use of chemical weapons. This incident, and the states' responses to it, suggest support for the approach discussed in this article for assessing the legality of different uses of force.

In other historical incidents of states using limited armed force, the states involved have also failed to invoke article 2(4) of the Charter. As an illustration, the forcible abduction

of Adolf Eichmann from Argentina in 1960 by Israeli intelligence was found by the UN Security Council to be a violation of Argentina's sovereignty. The Argentina delegate to the UN never invoked article 2(4) nor did the Security Council in its resolution. [72] In contrast, the abduction of General Noriega in Panama in 1989 following the US invasion, was considered in the context of the gravity of a military invasion of another state and not the individual abduction of one person. In short, a forcible abduction may or may not constitute a use of force depending on the full context of the case and the gravity of the force used. [73] For these kinds of forcible enforcement measures that are not covered by article 2(4), and therefore do not constitute an unlawful use of force, they may still constitute violations of other legal obligations, such as the obligation not to intervene in the affairs of another state or breaches of other specific treaties. [74] These minor armed uses of force fall outside the scope of article 2(4), based on the context and domain in which they occur and their gravity, and while potentially implicating other regimes of law (international criminal law, sea and air law) they would not violate the Charter.

Applied in the cyber context, according to this "minimum use of force" standard for the use of force, a "cyber operation that causes minimal damage in another state's territory such as the destruction of a single computer or server," with no hostile intent towards the state itself, and without further effects, "would clearly not fall within the scope of the provisions" of article 2(4) under the minimum use of force test. [75] In applying the *de minimis* standard, the quantity of force matters as well as the context of the incident. Such an operation that involves the destruction of property in another state, would, however, impose effects within another state's territory and, if coercive, in the sense of intended to compel a state to behave in a manner other than how it would normally behave, be an unlawful intervention. [76] According to the then-legal advisor to the U.S. Department of State, Harold Koh, in discussing some of the factors that would be relevant to a legal assessment of actions involving uses of force in cyberspace, he specifically included "intent" and gravity, among others, to be taken into consideration. [77] Ultimately, whether a minimum use of force will constitute a violation of article 2(4) will depend on the specific circumstances of each case.

Analyzing the meaning of a "use of force" in this more limited manner affords a state subject to a use of force in violation of article 2(4) more options for legally responding than the state would have under an approach accepting a broader meaning of a use of force under article 2(4). Under a broad interpretation of article 2(4) uses of force, and a broad interpretation of the *Nicaragua* Court's findings, to be discussed in more detail in the next two sections, a victim state would be prohibited from using forcible responses unless the attack against the state rose to the high threshold of an armed attack. In contrast, with a limited interpretation of article 2(4), states that are targets of uses of force violating article 2(4) but not constituting an armed attack under article 51 of the Charter can conduct forcible responses as long as such responses are of a *de minimis* nature or gravity both in its objectives and its means. Such forcible responses would fall outside of the

article 2(4) prohibition and would constitute permissible countermeasure [78] even though they may cause minor physical harm, injury or damage in the state's territory. [79]

An example of a cyber operation that would not necessarily be covered by article 2(4) could include the disruption of Internet service that, although possibly involving the violation of certain economic rights or property rights under international law, would not be covered by article 2(4) based on the gravity of the effects and the full context of the situation. Other actions not covered by article 2(4) could include, for instance, the interruption of the production lines of a manufacturing company in another state through Internet-facing network connections that would involve hacking into the manufacturing control units and robotics and potentially causing them to produce faulty manufacturing or physically destroying the manufacturing equipment itself. Although likely to violate other laws such as international criminal law, depending on the context and gravity of effects, they may not be covered by article 2(4) and therefore could constitute lawful countermeasures if done in response to a wrongful act and complying with the other requirements for countermeasures such as proportionality that will be discussed below in more detail. [80] In contrast, if a broader interpretation of article 2(4) is accepted, expanding article 2(4) to include all uses of force, any proportionate forcible response, even in-kind, to a use of force would be in violation of article 2(4) and a prohibited forcible countermeasure.

Article 51 Self-Defense Exception to the Prohibition on the Use of Force

Under the Charter, the article 2(4) prohibition on the use of force was subjected to two explicit exceptions: military action authorized by the UN Security Council following a determination of 1) the existence of a threat to the peace, a breach of the peace, or 2) an act of aggression, and self-defense in response to an armed attack. As an exception to this prohibition, states may use force if the UN Security Council authorizes it pursuant to its responsibility to maintain peace and security; this includes the authority to respond to threats to the peace, breaches of the peace, and acts of aggression. [81]

The article proclaims:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. [82]

As a matter of customary law, a state can also use force in self-defense if an armed attack is imminent but has not yet occurred. [83] The article 51 principle of self-defense reflects customary international law and has been recognized by states as applying to defense against cyberattacks that are equivalent to armed attacks under article 51. [84]

As an exception to the prohibition on the use of force, a state can employ forcible cyber operations in response to an armed attack that has occurred or is imminent [85] as long as the forcible defensive measure targets the responsible state or non-state actors [86] and

complies with the customary legal principles of proportionality and necessity, as discussed later in more detail.

Distinguishing an Article 51 Armed Attack From an Article 2(4) Use of Force

Interpreting the rule of self-defense for cyber within article 51 requires an understanding of the meaning of the term "armed attack," that, like the term "force" as used in article 2(4), remains undefined in the law. The ICJ in the *Nicaragua* case, without providing a specific definition for an armed attack or use of force, drew a distinction between the two terms and developed a "gap" theory, where only the most severe or grave uses of force would constitute an armed attack, utilizing a "scale and effects" standard to distinguish between a use of force and the gravest uses of force that would constitute armed attacks. [87] In other words, a certain degree of armed force could meet the gravity threshold of article 2(4), nonetheless fail to trigger the higher threshold for article 51 self-defense if the armed force was not sufficient enough.

Based on this "scale and effects" test utilized in the *Nicaragua* case, isolated or minor incidences that do not threaten the safety of the state, while hostile and unlawful, would not constitute an armed attack reference to the Charter's right of self-defense. If, however, the results of the armed force met the gravity threshold, resulting in or imminently resulting in a considerable loss of life or extensive destruction of property, it would constitute an armed attack under international law, triggering the victim state's right to use lethal force in response. There is a minority view among some states and legal experts, including the US, that there is no distinction between a use of force and an armed attack, and that any unlawful use of force qualifies as an armed attack triggering the right of self-defense. The US has taken this position with respect to cyber operations as well. [88] While disagreements persist between states and commentators as to the validity of a gap between the thresholds and the nature of any gap that may exist, state practice has supported the position that kinetic operations causing significant physical damage, injury or death would qualify as a grave use of force and therefore an armed attack; this reasoning has been extended to cyber operations. [89]

Since *Nicaragua*, government officials and scholars have struggled to define the precise threshold at which a use of force would constitute an armed attack, finding "[I] t is almost impossible to fix the threshold of force employed to define the notion of armed attack," and failing to develop a bright-line test. [90] Disagreement continues to exist as to whether the 2010 Stuxnet operation against the Iranian nuclear program that damaged over 1000 centrifuges, qualified as an armed attack. [91] In accordance with *Nicaragua*, a use of force would constitute an "armed attack" only when both the *scale* and the *effects* of the use of force were grave enough. For the sufficient *scale* to be met under this test, considerable magnitude and intensity must be involved, taking into consideration the amount of force used and duration of the attack. For the threshold of *effects* to be met, the consequences

have to involve substantial destruction to important elements of a state, namely, its people, territory and, in certain cases, its economy that compose the security of the state. Even in cases where armed force is used and causes damage, unless it is of a high enough intensity, it will not constitute an armed attack. In finding that mere "frontier incidents" using military force do not have the necessary gravity to be considered armed attacks, the ICJ supported this position. [92]

This aspect of the Court's decision has faced much criticism in that the gap created by the Court between permissible self-defense and lower level attacks by armed bands served to reduce the barrier to armed aggression because it took away the military deterrent from lawful recourse to self-defense. [93] The decision was further criticized for not elaborating on the required scale and effects necessary to reach the threshold of an armed attack nor what type of response might be appropriate for acts that fall below the threshold. In its opinion, the Court indicated that the threshold of gravity is a flexible one dependent on the specific circumstances of each case. For example, in contrast to the example of "frontier incidents" in the *Nicaragua* case, in accordance with the same scale and effects standard developed by the Court in another case with a different set of facts, the Court "[did] not exclude the possibility that the mining of a single military vessel might be sufficient to trigger the 'inherent right of self-defence." [94] Therefore, even a single incident of armed force that leads to a considerable loss of life and extensive destruction of property would be of sufficient gravity to constitute an armed attack. [95] In the context of cyberspace, a single cyber operation against computer systems that caused a significant number of fatalities would likely constitute an "armed attack." [96]

For cyber operations that do not result in direct physical damage but result in destructive second-order effect, there is growing support based on the stated opinions of governments that such actions may constitute not only uses of force but also armed attacks under the Charter framework. [97] As states have come to recognize the vulnerabilities of critical infrastructure to cyberattacks that could inflict substantial destruction to critical elements of a target state (its people, economy, and security infrastructure) international jurists and governments have concluded that disruptive cyberattacks against such infrastructure, although not causing direct physical damage to the infrastructure, nevertheless of the requisite magnitude resulting in significant damage to the nation or its people, versus mere inconvenience, could constitute an "armed attack," triggering the legal right to use forcible responses in self-defense. [98] For example, a cyber operation that interrupts the cooling functionality of a nuclear reactor, while not destroying the reactor causes the cooling system to malfunction, leading to the release of radioactive materials and the loss of life, would result in significant enough second-order effects that amount to an armed attack irrespective of the fact that the initial cyber operation did not produce direct harmful or permanent effects to the reactor. [99] In cases of cyber operations that cause no

physical damage but severely incapacitate critical infrastructure, such as banking institutions, if the effects are serious enough, may constitute an "armed attack." [100]

In line with the "scale and effects" approach, only armed attacks will trigger the right of self-defense and therefore all other attacks or hostile actions by states that fall below this threshold are classified as uses of force, interventions or general violations of sovereignty, depriving the target state of such attacks the right of forcible self-defense under article 51. This standard of scale and effects, however, is a "variable standard" [101] which does not require it being applied separately to each hostile act, but instead can be applied in combination with multiple acts to meet the high threshold of an armed attack. The Court has implicitly accepted this approach, the doctrine of "accumulation of events," in particular circumstances where consecutive attacks take place that are linked in time, source and cause, and are part of a "continuous, overall plan of attack purposely relying on numerous small raids." [102] In such cases where there may be some small-scale uses of force falling below the level of an armed attack, collectively they can amount to such an armed attack. In this context, cyber operations against a state that would in themselves merely constitute "less grave uses of force," when forming part of a chain of events carried out by the same source, can qualitatively transform into an "armed attack" triggering the right of self-defense. [103] The question remains, however, as with assessing the gravity threshold for singular armed attacks, how many individual lesser grave uses of force are required to constitute an armed attack?

Given that the most common form of cyber force between states has been a stream of low-intensity cyber operations versus actions at the armed attack level, this doctrine of accumulation of events in the context of self-defense may be relevant. [104] Under this doctrine, in circumstances where there are a number of "less grave uses of force" that take place either exclusively in the cyber domain or different domains (cyber and kinetic) that can be linked together to form part of a chain of events by the same state, the nature of the acts taken together could amount to an "armed attack," triggering the right of self-defense.

Self-Defense Responses to an Article 51 Armed Attack

The right of individual or collective self-defense referenced in article 51 of the Charter is the right of a victim state to use offensive force against a state legally responsible for an armed attack to prevent or stop harm to the state or its allies. [105] All self-defensive actions, to include cyber operations carried out in self-defense, must be proportionate and necessary. Necessary responses in self-defense are those actions that are used as the last resort and have been determined to be the only means by which to repel an attack or prevent a subsequent attack. [106] Proportionate responses are those that are in balance against the purpose of repelling the attack to end the situation or threat, which caused the attack. [107] Proportionate self-defense responses can be quantitatively greater than the initial armed attack since it aims to repel that attack. [108] In other words, if the threat continues after an

initial armed attack, the victim state can use all necessary force to eliminate the threat. Beyond just intercepting the immediate armed force, the victim state could use deadly force to degrade the attacker's military capabilities or seize territory in order to assure its future security against the attacker, imposing a higher level of cost to the adversary than the initial attack imposed, so long as it has been determined that such a level of force is required to stop the threat. [109] What matters in assessing the proportionality of a self-defensive action then is "the result to be achieved by the defensive action and not the forms, substance, and strength of the action itself." [110] The right of self-defense has been recognized to extend to cyber operations that rise to the level of an armed attack. [111] If forcible cyber operations meet these standards for self-defense they would be lawful.

In determining an appropriate legal self-defense response, attribution is key. It does not matter where an armed attack occurred, [112] what type of weapon was used to carry out the attack, [113] whether the target was civilian or military, or how many individual incidents occurred. [114] As long as the victim state can identify the responsible state for the attack and the overall effects of the incident or incidences reach the high threshold for an armed attack, the victim state can act in self-defense against the responsible state. For example, if a state carries out an attack, whether by a kinetic or cyber operation, against a civilian computer system owned and operated by a private company within the territory of another state that causes a devastating impact, although it has no connection to military or government entities, such an attack will constitute an armed attack for purposes of article 51. [115] Neither the nature of the attack as a cyber operation nor the governmental or private nature of the target is relevant to the determination of the existence of an armed attack against the state in its territory. [116] In responding to an armed attack, actions are not limited to in-kind methods; for instance, reactions to cyberattacks that constitute armed attacks could be exercised by physical, cyber, or other means. [117] Furthermore, there is no requirement under international law for states to publicly disclose the basis for its attribution assessments. [118]

Defensive Self-Help Responses to Hostile Actions Below the Threshold of Armed Attack

Historically, defensive self-help involved retaliatory measures by a state against another state that had violated its rights protected by international law. The idea of such measures was based on a lack of centralized enforcement in the international community and, therefore, self-help measures played an important role in bringing about a situation that conformed to the law. The recognized value of such measures "lay in the possibility of gaining redress without creating a formal state of war." [119] With the modern development of international law within the Charter, article 51 established forcible self-defense as a separate institution from self-help, making armed force in self-help mostly forbidden except for the occasional resort to *de minimis* forms of force due to the ineffectiveness of the UN Security Council to enforce the law. [120] Under the old concept of self-help and the right of states

to wage war, a state's recourse was practically without limitation and covered retorsions, reprisals, both armed and peaceful, peaceful blockade, intervention, and even war. Today, self-help still includes retorsions, countermeasures, and necessity, which are all remaining legal options for states to act unilaterally for coercive enforcement of rights, albeit with a number of restrictions.

As international law provides states with options for responses to hostile actions below the article 51 threshold in the physical domain, so too does the law permit victim states to respond to unlawful actions that fall below the armed attack threshold. Especially in an era where states are pursuing their strategic objectives and coercively operating in the gray zone, victim states will find relief as international law does not leave such states powerless to defend against and respond to such gray zone cyber threats. As recently expressed by the then-nominee for Commander, U.S. Cyber Command, "Although cyber operations not involving loss of life or significant destruction of property may not constitute an armed attack those operations causing significant impact on U.S. foreign and economic policy interests may nonetheless violate international law and trigger U.S. response options." [121] Indeed, customary law has provided multiple options for victim states to respond to offensive measures by other states, short of war or an armed attack, whether the measures are conducted in cyber or not.

For those states that are victims of coercive or forcible cyber operations that fall short of an "armed attack" in article 51, recourse can be taken unilaterally, to include the adoption of retorsions and countermeasures and measures invoked under a plea of necessity that do not reach the "armed attack" threshold. [122] According to the *Articles of State Responsibility* (Articles) drafted by the UN International Law Commission (ILC), [123] countermeasures and actions of necessity are measures that would otherwise not be justified under the law but for, in the case of countermeasures, a prior wrongful act against the state, and in the case of acts of necessity, exigent circumstances where the state's essential interest are in "grave and imminent peril." [124]

Given the role that the Articles will play in assessing state responsibility for cyber activities, some background on the Articles is relevant. In 2001 over forty years of work of the ILC on state responsibility was concluded with the adoption of fifty-five draft articles. Unlike the ILC's previous projects, the work did not result in a treaty but rather in draft articles that were "taken note of" by the UN General Assembly, indicating the challenges with reaching agreement on the Articles during the drafting process and concluding without universal state agreement. Although the Articles are not a binding source of law, they can serve as a source of ascertaining the law, similar to the writings of highly qualified publicists, and indeed, some aspects of them have been accepted as customary law by international tribunals and at least some state practice has provided evidence of its customary characteristic. [125] Some provisions of the Articles, however, were controversial

during the drafting and still are, particularly the articles on countermeasures, leaving the status of those provisions under the law uncertain as they have not been accepted by states as authoritative restatements of customary international law. [126] Related to the work of assessing the legality of cyber operations, the *Tallinn Manual 2.0* relied heavily on the Articles in developing some of its rules. Given the lack of clarity and controversy over some provisions of the Articles, it may be that with respect to the Tallinn Manual's rules that are based on these same provisions, more work will need to be done by states and possibly judges before the law is clear in this complex area.

For assessing state responsibility, as the Articles did, it is useful to first distinguish countermeasures (previously called reprisals) [127] and pleas of necessity from retorsions under international law. An act of retorsion is a coercive, politically unfriendly, but lawful act, not involving any breach of international obligations owed to the target state, whether treaty-based or customary and thereby do not require any legal justification. [128] States can undertake cyber or non-cyber retorsions at any time to influence another state's actions, regardless of whether there was a prior law violated or any detrimental effects to the interests of the targeted state from the retorsions. [129] Although retorsions can be taken at any time and have few, if any, restrictions because of their legality, typically, they are taken in response to a breach of an international legal obligation owed to the state. Common examples of retorsions include protests and verbal condemnation or diplomatic demarches, discontinuing development aid, denying entry visas, declaring that a diplomat is *persona non grata*, imposing travel restrictions on foreign nationals within the state, terminating cultural and educational exchanges, and imposing unilateral sanctions. [130]

Recent examples of retorsions conducted by the US in response to cyberattacks have included unilateral sanctions against North Korea in response to the Sony cyberattack [131] and against Russia in response to its cyber operations against the Democratic National Committee and related interference with the 2016 US election. [132] In addition to sanctions, the US expelled Russian diplomats from US territory, also constituting a retorsion. [133] These US actions were lawful, although considered unfriendly, and could have been done irrespective of the unlawfulness of the cyber operations conducted by North Korea and Russia. [134] An example of a *cyber* retorsion would be a state selectively blocking, at its own gateway, another state's Internet traffic from entering the territory, provided such action did not violate any existing treaty agreement between the states or any customary law. [135]

In contrast to retorsions, countermeasures are actions, short of armed attack, or omissions that breach an international obligation owed the targeted state and therefore are unlawful except for a prior law violation by the targeted state. [136] The purpose of countermeasures is to compel the responsible state to comply with its international obligations owed to the injured state and make reparations for the injury caused. [137] While countermeasures have been established through international practice and decisions from

tribunals and courts as a circumstance precluding wrongfulness, the legal regime applicable to countermeasures is far from well-established as states have objected even during the drafting of the *Articles of State Responsibility* to different aspects of the Articles as they apply to countermeasures in particular. In the comments the US submitted to the ILC during the drafting process emphasis was placed on the US objections to the restrictions on the use of countermeasures that were included in the Articles. [138] This may indicate that for certain aspects of the regime of countermeasures, the Articles, and potentially the rules on countermeasures in the *Tallinn Manual 2.0,* are more a progressive development of the law, rather than the codification of existing customary rules. Indeed, the topic of countermeasures was one of the contentious issues in the discussions of the 2017 UN GGE that failed to reach a consensus report. [139]

According to the *Articles of Responsibility,* an injured state that has suffered a wrongful act by another state may commit a wrong in reaction, a countermeasure, as long as it is "commensurate" with the injury suffered from the initial wrongful act, taking into consideration the rights in question [140] and the state's response is aimed at inducing an end to the initial wrong, and the provision of damages for injuries suffered. [141] Despite the clear nature of the requirement of a prior wrongful act, there remain some unresolved issues related to this requirement for countermeasures. For example, due to a lack of state practice and no treaty-based clarification, the specific issue of whether a state that conducts countermeasures must be directly injured is of great debate with opposing views. [142] The question being, does the state that is conducting the countermeasure have to be the state that suffered the injury from the wrongful act. This issue of individually or collectively conducted countermeasures, irrespective of individual injury, in defense of another injured state or in respect of breaches of obligations *erga omnes,* has yet to be resolved, leaving open the further development of the law through state practice and *opinio juris* and the possibility for collective, or third-party, cyber countermeasures. [143]

Another contentious issue that remains unsettled is whether a state can conduct forcible proportionate countermeasures that would violate article 2(4) of the Charter in response to forcible actions that are below the article 51 armed attack level of the Charter. [144] While there is widespread agreement that countermeasures must not be of the severity of an armed attack as meant by article 51 of the Charter, the debate remains over the allowable level of force of countermeasures. [145] According to the ILC, "questions concerning the use of force in international relations . . . are governed by the relevant primacy rules" and not by the law of state responsibility. Following this reasoning, the *Articles of State Responsibility* provided no guidance on the specific question of whether forcible countermeasures that triggered article 2(4) would be *per se* illegal, leaving it for analysis under the Charter. On the one hand, some commentators have argued that based on the dicta in *Nicaragua*, the ICJ seems to have "implicitly left open the door for proportionate forcible

countermeasures" in the case of a victim state suffering from hostile acts that are not at the threshold of an armed attack. [146] On the other hand, commentators have argued that the obligation to refrain from the use of force under the Charter has been recognized as a limitation to countermeasures. [147] The *Tallinn Manual* experts were unable to reach agreement on this point and therefore offered no rule prohibiting the use of force countermeasures that would violate article 2(4). [148] Interestingly, one of the ICJ judges recently provided an interpretation of the Court's opinion with respect to countermeasures, one that is in contrast with previously offered interpretations. At a celebration of the ICJ's anniversary, Judge Yusuf stated, in referring to the *Nicaragua* case, "[T]he Court did not specify the nature of such 'countermeasures,' but it could perhaps be reasonably assumed that it was referring to military countermeasures." [149] One reasonable understanding based on the Judge's interpretation of the Court's opinion would be that lawful countermeasures may include the armed force that would violate article 2(4). Another understanding of this interpretation is that countermeasures could include armed force that was never meant to be covered by article 2(4).

Perhaps a more effective way to address this debate would be to adopt a more limited meaning of what a use of force is under article 2(4). In using this approach, as discussed earlier, one could argue that there are uses of armed force that do not enter the scope of the Charter's article 2(4) because of the low intensity of the force involved, and the context of the use of force. Rather than article 2(4) as the relevant law for those actions not covered, the focus would be on other legal regimes that may be relevant to the context of the situation. Using this standard of a more limited view of the meaning of use of force in article 2(4) would alleviate the tension over whether countermeasures can be forcible since by allowing for minimal force that is not prohibited by article 2(4), countermeasures could involve force of a minimal level that would not violate article 2(4) and therefore would be lawful under the law of countermeasures. [150] This would also allow states that are victims of uses of force that violate article 2(4) but that do not rise to the level of an armed attack to take forcible action, albeit limited in scope and intensity, in another state's territory as long as it is proportionate to the injury and intended only to get the state to comply with its obligations. Rather than limiting the victim state to non-forcible responses that may not be effective in getting the wrongful state to comply with its legal obligations, under a more limited meaning for article 2(4) uses of force, a state may use forcible proportionate countermeasures, including cyber countermeasures. Such cyber responses would be allowed whether or not the initial wrong exhibited through cyber operations or otherwise. [151] While these actions may violate the sovereignty of the state or other bodies of law, they would not be violations of article 2(4).

In choosing what countermeasures to employ, the state has considerable flexibility in choosing which obligations to violate vis-à-vis the other state, without publicly disclosing

the basis for its attribution assessment of the prior wrongful acts of the targeted state to the targeted state. The state conducting the countermeasure ought to take care that its attribution is accurate to avoid any political consequences. If, however, the acting state in taking countermeasures was mistaken as to fact or law, and, for instance, employs countermeasures against a state that has not conducted any wrongful act, such countermeasures may still be considered lawful. Although this issue of responsibility for a mistake is a debatable point in international law, some have argued that since there is no general principle under international law as to a "fault standard in the commission of a wrong" nor is international law a system of strict liability, such countermeasures taken in error, if based on good faith, will be excused. [152] The claims and counterclaims of states after incidents of uses of military force made in error that were not considered wrongful, often settled with an apology, as well as the decisions of tribunals in relation to countermeasures, have suggested that states may be excused for countermeasures taken in error but based on good faith. [153] The opposing view, accepted by the ILC and the *Tallinn Manual* is that those states taking countermeasures "do so at their own risk" and will incur responsibility if in relying on erroneous facts or legal interpretations the state conducts an illegal countermeasure. [154]

In accordance with judicial precedence and the *Articles of State Responsibility,* there are a number of substantive and procedural requirements for countermeasures. [155] One such substantive requirement is that the countermeasure's sole purpose must be to get the offending state to comply with its international obligations, discontinue its wrongful acts and/or provide reparation; therefore, the use of countermeasures to punish or retaliate is prohibited, can only be taken once a wrongful act has taken place, not in an anticipatory manner, and must end when the state has complied with its obligations, which could include making reparations. [156] In seeking compliance by the wrongfully acting state, the state carrying out the countermeasures, when feasible, should give notice of its intent to use countermeasures, [157] hereby providing the state an opportunity to comply. This preference for notice, however, has been interpreted as not mandatory and will depend on the particular circumstances. [158] If, for instance, giving notice would result in a less effective countermeasure then notice would not be required. [159] In addition, because the purpose of countermeasures cannot be punitive, the measures taken should be reversible, if possible. [160]

While countermeasures must be targeted only at the state responsible for the wrongful act, [161] this requirement does not prohibit countermeasures against private entities within that state in order to get the state to change its behavior and comply with its legal obligations. [162] Importantly, especially in the context of cyber countermeasures where actions may inadvertently impact third states, such effects, as long as there is no breach of a legal obligation owed to the third state, would not result in the countermeasures being unlawful. [163]

Commonly cited examples of non-forcible countermeasures that states have employed include the seizure of assets of foreigners, trade embargoes, and breaches of treaties such as bilateral aviation agreements. Examples of non-forcible *cyber* countermeasures could include "blocking electronic access to a state's bank accounts" contrary to an applicable treaty provision. [164] Measures that have been characterized as countermeasures with minimal force, not covered by article 2(4) under a *de minimis* or gravity threshold approach, include shooting across a ship's bow in response to violations of fishing quotas, forced landing or shooting of an aircraft within a state's airspace without authorization, abduction of criminals in another state's territory without consent, and the rescue of nationals abroad. [165] As long as it has been determined that these actions would be proportionate to the injury that was suffered, taking into consideration the principles at stake from the wrongful act, such countermeasures carried out by cyber means would be lawful since they do not constitute a violation of article 2(4).

Under the *de minimis* standard for article 2(4), an example of a lawful forcible *cyber* countermeasure involving minimum force could involve the disabling of Internet access routers of a state within that state's territory, denying the state access to the Internet. While this action may constitute a violation of the state's territorial sovereignty by the action taken in the territory of that state, it would not be covered by article 2(4) because of the *de minimis* nature of the force. In contrast, a cyber countermeasure that included the bricking or destruction of all routers in another state, causing irreversible damage to critical infrastructure, would likely be covered by article 2(4) and, reaching the requisite level of force, would not be permissible under the law of countermeasures.

In circumstances where a state's reply to hostile cyber operations cannot be justified as a lawful countermeasure, for instance, if such measures would fail to meet any of the requirements for countermeasures, the state could still act to prevent imminent or ongoing hostile cyber operations that represent a "grave and imminent peril" to the "essential interests" of the state pursuant to a "plea of necessity." [166] Although the plea of necessity was once considered "marginal," there is substantial authority for its existence from state practice and international tribunals that have either accepted the principle as a circumstance precluding wrongfulness or at least not rejected it as such. [167] Similar to countermeasures, this concept of necessity, although not anchored in any conventional provision of law but being in principle accepted by a growing number of states, permits a state to escape liability under the law of state responsibility for its actions that would normally constitute a violation of international law, whether a treaty or customary obligation. [168]

While there is a recognized trend that this defense of necessity is "now coming to the forefront of public international law, suggesting that more and more states will argue necessity in the future. . .," [169] necessity is controversial and has only been accepted as an exceptional rule. In the 19th and 20th centuries, concerns raised about states abusing

necessity by using it as a pretext to justify armed attacks against other states, resulted in the development of stringent requirements for the plea designed to carefully constrain the doctrine to a narrowly defined set of circumstances. [169] Today, it remains unsettled as to whether necessity can be invoked to justify forcible actions that would violate article 2(4) of the Charter, both in the context of traditional military kinetic operations as well as cyber operations. [170] However, for actions under a plea of necessity, just as with countermeasures, that are forcible but not covered by article 2(4) because of their limited intentions and purposes which bear no relation to the purposes characteristic of true uses of force as meant by article 2(4), such actions under necessity could be justified.

As distinguishable from the conditions required for countermeasures, the conditions for the application of necessity can be divided into two categories. The first category relates to balancing conflicting interests at stake and includes four constitutive elements: a) an essential interest of the state invoking the necessity is at stake, b) an interest is threatened by a grave and imminent peril, c) the action must be the only means to guard against the peril, and d) the interest to be disregarded in taking the action must be of lesser value than the interest being safeguarded. The second category includes circumstances of an absolute preclusion to invoking the defense: when the primary rule at issue, such as the use of force regime of the Charter, excludes the possibility of invoking the principle and when the state whose interest is threatened substantially contributed to the occurrence of the situation of necessity. [171]

Although there is no accepted definition of what would constitute "essential interests" of a state under international law, examples from international cases and state practice have included issues related to a state's security, the preservation of the state's natural environment or the ecological equilibrium, economy, public health, safety, and maintenance of the food supply for the population. [172] As to the element of grave and imminent peril, what is required is that the "peril is clearly established on the basis of the evidence reasonably available at the time" [173] and the prohibited actions taken are to be "the only way for the State to safeguard" its essential interests, leaving no other legitimate choices left for the state. [174] The actions must also not affect the vital interest of any other state in a grave and imminent way. [175] In other words, the interest sought to be protected by the state in conducting the actions under the plea must be of greater importance than the other state's interest that will be temporarily disregarded.

In contrast to countermeasures and self-defense, actions based on necessity do not require any initial wrongful act, and therefore attribution is not necessary. [176] In the cyber context, given that attribution challenges persist, this may make necessity particularly useful in the face of grave threats through cyberspace. Furthermore, unlike countermeasures, which cannot be invoked in anticipation of a legal obligation being breached, actions

under necessity can take place before the culmination of the grave threat to the state's interests, anticipating the grave harm that will ultimately emerge. [177] As a cautionary note, actions under necessity have been found by courts to be permissible only under what is considered exceptional circumstances when the situation constitutes a grave and imminent peril to the essential interests of the acting state. [178]

Although the standard for invoking necessity is high and circumstances allowing it are exceptional, the nature of state cyber operations, in particular, those targeting critical infrastructure, may be the circumstances that meet the high standards for necessity. In cyberspace where threats can materialize almost instantaneously through the Internet, bringing to a halt the functions of critical infrastructure that support essential state functions, target states may not have the time to seek cooperative measures from other states from which the threats emanate, or transit through, or obtain provisional measures from a Court, to eliminate the threat. Furthermore, the states whose territory is impacted by the impending peril may lack the means to take effective measures to stop the situation. As an example, consider the case of highly disruptive cyber operations against a state's banking system that would result in the loss of critical financial services and commerce to a state's population. In this situation, to prevent the harm, the state may need to respond immediately, without first attributing the attacks, and block access to some of its infrastructure from specific countries which it has existing treaty obligations with that guarantee access to the relevant infrastructure. In such a case, a justified action based on necessity could include blocking access within the responding state or if necessary in the territory of the other state from which the operation is emanating.

In a different context where a state discovers malware on a gas pipeline control system in its territory, malware that is preprogrammed to be activated in the future that will result in the disruption of the system, preventing the pressure relief function from properly working and potentially leading to a rupture of the pipeline that would jeopardize the safety of the pipeline workers and the surrounding civilian population, actions under a plea of necessity would likely be justified. In this case, it may be that in conducting its cybersecurity operations, the pipeline company finds and removes all of the malware that can be removed while keeping the system operational but locates other malware that cannot be removed without shutting down systems that are critical to the safe operation of the pipeline. In this case, the state could invoke the plea of necessity and take actions to eliminate the threat or allow the company to take such actions. It may be necessary to take action beyond the state's borders as the only means of preventing the malware from triggering and disrupting the pipeline operations. In the case where the blocking of IP addresses would not be sufficient to prevent the impending harm, and there is no time or means for the state from whose territory the command and control servers reside to take the necessary measures, or the state is unwilling to take the necessary steps, a cyber response under a plea of necessity could entail hacking back and shutting down cyber infrastructure

in that territory that is being used to mount the harmful operations as long as by doing so would not seriously impair the essential interests of any affected state. [179] In the face of the grave and imminent, and otherwise, unavoidable danger to the essential interests of the state from the pipeline failure, the state would be justified in violating its international obligations owed to the other state.

In cases of cyber operations targeting critical infrastructure that would result in "severe negative impact" on the target state's "security, economy, public health, safety, or the environment," the necessity plea is available to states as a last resort and may be particularly relevant given the nature of cyberspace and hostile cyber operations and the international rules related to the use of force and state responsibility. [180] In circumstances similar to the pipeline example where logic bombs are found on networks and attribution for the implants is not possible or time does not allow for it, countermeasures will be unavailable. Furthermore, given that current uncertainty about if and how the general principle of sovereignty applies to cyber activities, in particular to unconsented territorial interference in computer networks of another state, [181] the issue of the legality of implanting malware in another state's infrastructure is left unclear, thereby leaving countermeasures unavailable without a clear prior wrongful act in the case of implanted malware. Under these circumstances, the plea of necessity may present the only lawful option for the state in preventing the harm to its essential interests.

CONCLUSION

Traditionally, international law maintained a strict division between war and peace, holding *inter bellum et pacem nihil est medium* – there was no intermediate state between war and peace. [182] Of course, in those times it was seldom difficult to determine whether armed force was being employed, triggering a state of war, and which state's forces were involved. Describing a very different security environment today, the 2017 *U.S. National Security Strategy* (NSS) warns that the factual dividing line between peace and war has become more difficult to determine, describing current international relations as more of "an arena of continuous competition." [183] As the former British Secretary of State for Defense recently declared, contemporary adversaries are deliberately seeking to "blur the lines between what is, and what is not, considered an act of war." [184]

Although determinations of the facts on the ground may be more challenging in the context of cyber operations, where technological developments and networked communications have allowed states to more easily use proxies to disguise their actions, enabling their hostile actions to remain below a level that would provoke a full-scale response, the Grotian divide between war and peace still remains a vital part of the international legal order in support of international stability. Key to the Grotian notion, however, is clarity about the legal thresholds that divide peace from war as well as the redlines for

the legality of actions during both times of peace and times of war. But as the NSS points out, adversaries are exploiting existing international law principles that are ambiguous or subject to competing interpretations in all domains as they operate on the edge between peace and war. In doing so, they hope to avoid any serious consequences for violating the laws that have developed through treaties and custom. Efforts to counter these threats will require addressing these legal ambiguities that are currently inhibiting state responses and allowing violators to escape repercussions.

As international law is sure to evolve as it has done historically in the face of new threats and technologies, it will be for states to drive this evolution. Whether they will eventually consent to rules within a treaty for cyber operations or not remains to be seen. The law, however, will also evolve through the consent of states in their practices out of a sense of legal obligation, *opinio juris*, which can eventually crystallize into customary international law. Coupled with the decades of state practice of employing cyber operations in their strategic and military activities, the recent public statements by government officials concerning the interpretation of international law as applied to those cyber operations serve to develop and reaffirm interpretations of international rules, tailoring them for this domain. [185] These trends will help address the gray zone conflicts, including the cyber operations that are part of those conflicts, and diminish the advantages adversaries are seeking to gain in this space. In doing so, states will shrink the area of gray zone conflicts, providing fewer opportunities for states to exploit gray zones, and generate much-needed stability in cyberspace, support for the development of effective frameworks for national policy, doctrine and rules of engagement for cyber operations, and enhanced deterrence within the global cyber domain. [186].

NOTES

1. Ellen Nakashima, "When Is a Cyberattack an Act of War?" *The Washington Post,* October 26, 2012, https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html?utm_term=.79f2f366be90.

2. Morgan Chalfant, "Democrats Step Up Calls that Russian Hack Was an Act of War," *The Hill,* March 26, 2017, http://thehill.com/policy/cybersecurity/325606-democrats-step-up-calls-that-russian-hack-was-act-of-war.

3. Mark Pomerleau, "Intelligence officials: Cyber domain is still the 'Wild West'," *Cyber Defense,* 2015 (quoting testimony from Deputy Secretary of Defense Robert Work before the Senate Armed Services Committee stating, "[T]here's no defined red line for what would constitute an act of war."), http://defensesystems.com/articles/2015/09/30/in-congress-cyber-wild-west.aspx. Mike Rounds, "Defining a Cyber Act of War: The Rules Regarding This Dangerous Threat Aren't Clear – Some Concision Is Urgently Needed," *Wall Street Journal,* May 8, 2016, http://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124.

4. Clyde Eagleton, "An Attempt to Define War," 291 *International Conciliation* (1933), 237, 281.

5. Yoran Dinstein, *War, Aggression and Self-Defence* (3d ed. 2001), 13 ("War is a hostile interaction between two or more States . . . in the technical sense is a formal status produced by a declaration of war . . . in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.")[hereinafter Dinstein, *War, Aggression and Self-Defence*].

6. U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,* January 2018, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

7. Speech by Valery Gerasimov, chief of the general staff of the Armed Forces of the Russian Federation, February 2013 ("In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."). Gerasimov's speech was translated by Robert Coalson and reprinted in his "Top Russian General Lays Bare Putin's Plan for Ukraine," *Huffington Post*, September 2, 2014; accessed February 19, 2018 at https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

8. U.S. Special Operations Command, *White Paper: Defining Gray Zones Challenges* 1, April 2015, https://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf. ("[G]ray zone challenges are defined as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."). See also, Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, 1-2 (Carlisle, PA: United States Army Way College Press, 2015) (defining gray zone conflicts where adversaries "employing gradual steps" remaining "below thresholds that would generate a powerful U.S. or international response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time . . . in the ambiguous no-man's land between peace and war . . .").

9. See Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," 42 *Yale J. Int'l. Law* 1, 2 ("The DNC hacks epitomized the grey zone strategy."). [hereinafter Schmitt, *Grey Zone*].

10. Statute of the International Court of Justice, Annexed to the Charter of the United Nations, 1945, 9 Int. Leg. 510, 522 [hereinafter ICJ Statute]. Treaties and customary international law are two of the main sources of international law. Unlike treaties that are negotiated and written by states, custom is generally non-written and comes into being when there is "evidence of practice accepted as law." ICJ Statute, art. 38.

11. For agreements by states as to the international norms and legal rules that apply to cyber operations see Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 24, UN Doc. A/70/174 (July 22, 2015) [hereinafter *UN GGE 2015 Report*]. The US has consistently stated its position that international law applies to state activities in cyberspace. See, U.S. Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* May 2011, 8-10. U.S. Department of Defense, Office of General Counsel, *Department of Defense Law of War Manual,* updated December 2016, (2015), 16.3.2 ("International law and long-standing international norms are applicable to State behavior in cyberspace.") [hereinafter *DoD Law of War Manual*]. See also, Brian J. Egan, Legal Advisor, Department of State, Remarks Delivered at Berkeley Law School, "Remarks on International Law and Stability in Cyberspace," November 10, 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf [hereinafter *Egan Speech*].

NOTES

12. Thomas M. Franck, *Fairness in International Law and Institutions,* 260 (1995). Similar to treaties, customary law is a primary component of international law. Under the standard view, customary international law is conceived of as having two components: an objective, state practice element, and a subjective, sense of legal obligation component, or *opinio juris.* International tribunals as well as state have endorsed this account of customary international law. See, e.g., *Jurisdictional Immunities of the State* (Germany v. Italy), (Feb. 3, 2012), ICJ 99, 122; *North Sea Continental Shelf Cases* (Fed. Rep. Ger. V. Denmark), (Feb. 20, 1969) ICJ 4, 44; Special Rapporteur, *Second Report on Identification of Customary International Law,* 9-10, Int'l L. Comm'n, UN Doc. A/CN.4/672, May 22, 2014.

13. Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum," 8 Harvard National Security Law Journal* (2017), 239, 242. ("While there is no longer any serious debate as to whether international law applies to transborder cyber operations, the international community has been unable to achieve consensus on the precise application of many international law principles and rules that govern them.") [hereinafter Schmitt, *Peacetime Cyber Responses*].

14. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, UN Doc A/68/98, (June 24, 2013), 8, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98. ("[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.").

15. See *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Michael N. Schmitt ed., 2013) (Cambridge: Cambridge University Press, 2nd ed. 2017) [hereinafter *Tallinn Manual 2.0*]. See also, Yoram Dinstein, "Computer Network Attacks and Self-Defense," *International Law Studies* 76 (2002), 103 [hereinafter Dinstein, "Computer Network Attacks"]. Marco Roscini. *Cyber Operations and the Use of Force in International Law* (2014) [hereinafter, Roscini, *Cyber Operations*].

16. See Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?," *Lawfare,* July 4, 2017, https://lawfareblog.com/un-gge-failed-internrnational-law-cyberspace-doomed-well. Michele G. Markoff, Deputy Coordinator for Cyber Issues, US Department of State, "Remarks as Prepared for The Chairman, UN GGE: Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," June 23, 2017, https://usun.state.gov/remarks/7880. See also, Catherine Lotrionte, "Geopolitics Eclipses International Law at the UN," *Cipher Brief,* August 6, 2017.

17. *Tallinn Manual 2.0. The Tallinn Manual* is a compendium of rules and commentary that were developed by international legal experts in assessing the applicability of international law to cyber operations. Although the rules do not reflect settled international law, and no state has accepted the rules generally as reflective of the law, the rules and commentary have garnered much international attention, and concern, justifying a close review of them. For an overview of the purpose of the Tallinn Manual project as well as analysis of some of its rules see Schmitt, *Peacetime Cyber Responses.*

18. The Hague Convention IV Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277; The Hague Regulations, Convention IV Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277. See also Ian Brownlie, *International Law and the Use of Force by States,* (1963), 80-83.

19. Covenant of the League of Nations, 225 Parry 195; 1 Hudson 1; 112 BFSP 13; 13 AJIL Supp. (1919), 128.

20. General Treaty for Renunciation of War as an Instrument of National Policy, August 27, 1928, 46 Stat. 2343, 94 LNTS 57 [hereinafter the *Kellogg-Briand Pact*].

21. See Lassa Oppenheim, *International Law* 225, 93 (Sir Hersch Lauterpacht ed., 7th ed. 1952).

22. See Mary Ellen O'Connell, ed., *What is War?: An Investigation in the Wake of 9/11,* Martinus Nijhoff/Brill Publishers, 9-10.

23. Jean Pictet, 9ed., *Commentary on the Geneva Conventions of August 12,* 1949, Vol. 1: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (ICRC, Geneva 1952) 32 ("Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2 [of the Geneva Convention], even if one of the Parties denies the existence of a state of war."); Marco Sassòli, Antoine Bouvier and Anne Quintin, *How Does Law Protect in War?* (Vol.1, 3rd edition, ICRC, Geneva 2011) 34 ("[A]s soon as the first (protected) person is affected by the conflict, the first segment of territory occupied, the first attack launched" then international humanitarian law starts to apply).

NOTES

24. See *Tallinn Manual 2.0*, Rule 82 and 83, at 290, for a discussion of the applicability of international humanitarian law to international and non-international armed conflicts in the cyber context. See also Michael N. Schmitt, "The Law of Cyber Warfare: *Quo Vadis," 25 Stanford Law & Policy Review*, 289-299 (2014) [hereinafter Schmitt, "Law of Cyber Warfare"].

25. *UN GGE 2015 Report.*

26. Kellogg-Briand Pact, art. 1; UN Charter, art. 2(4).

27. *Military and Paramilitary Activities* (Nicar. v. US), 1986 ICJ (June 27), 14, 99-100, [hereinafter *Nicaragua*].

28. See also, Yoram Dinstein, *War, Aggression and Self-Defence,* 94. *International Law Commission Yearbook,* 1966, 1966-II, 247, para. 1. In international law, *jus cogens* norms are those legal rules from which no derogation is permitted. See International Law Commission, *First Report on Jus Cogens,* Sixty-Eighth Session, UN Doc. A/CN.4/693, March 8, 2016 (prepared by Special Rapporteur, Mr. Dire Tladi).

29. UN Charter, Preamble, U.N.T.S., Vol. 16, 1 ff.

30. 6 Documents of the United Nations Conference on International Organization (1945), 339, 334–35; Conference on Int'l Org., S.F., Cal., April 25, 1945, Commission I: General Provisions, art. 7, para. 4.

31. UN Charter, art. 2(4).

32. See Albrecht Randelzhofer, "Article 2(4)," *The Charter of the United Nations: A Commentary* 106, 112-113 (Bruno Simma ed., 1995) [hereinafter, Simma, *Charter of the United Nations*]. See also Yoram Dinstein, *War, Aggression* and *Self-Defense* 88 (5th ed. 2011) ("the term 'force' in Article 2(4) must denote violence. It does not matter what specific means–kinetic or electronic–are used to bring it about, but the end result must be that violence occurs or is threatened.").

33. Mary Ellen O'Connell, "The Prohibition on the Use of Force," in *Research Handbook on International Conflict and Security Law* 89, 101 (Nigel D. White & Christian Henderson eds. 2013) [hereinafter O'Connell, *Use of Force*]. ("Excluded from the scope of Article 2(4) are such coercive measures as economic sanctions; diplomatic protest; physical force not involving weapons, such as cutting the nets of fishing vessels; disrupting internet service by denial of service attacks; and unconsented presence of official vessels or vehicles within another state's jurisdiction."). See also, *Corfu Channel Case* (UK v. Albania) (Judgment) (1949) ICJ Rep. 4, 35 [hereinafter *Corfu Channel*].

34. See Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Oxford and Portland: Hart, 2010) ("[W]hat matters, besides an abstract evaluation of the gravity of events [in assessing what is a use of force] is to determine whether there is an intention on the part of a State to use force against another State."), 201 [hereinafter Corten, *Law Against War*]. Corten's work is the most comprehensive account of state practice relating to the scope of "use of force" for the Charter purposes. See *Case Concerning Oil Platforms* (Iran v. US), Merits, Judgment, November 6, 2003, ICJ Reports 2003, para. 52, 61, 64 [hereinafter *Oil Platforms*]; *Nicaragua,* para. 231 ("Very little information is . . . . available to the Court as to the circumstances of these incursions or their possible motivations, which renders it difficult to decide whether they may be treated . . . as amounting, singly or collectively, to an "armed attack" . . . "). See also, Harold Koh, "International Law in Cyberspace," Speech at the USCYBERCOM Inter-Agency Legal Conference, September 18, 2012, in CarrieLyn D. Guymon (ed.), *Digest of United States Practice in International Law,* 2012, 598, http://www.state.gov/documents/organization/211955.pdf, [hereinafter *Koh Speech*] ("In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and *intent*, among other possible issues.") (emphasis added).

35. O'Connell, *Use of Force,* 102 ("Article 2(4) is narrower than it might appear on its face. Minimal or de minimis uses of force are likely to fall below the threshold of the Article 2(4) prohibition."). See also, Corten, *Law Against War,* 55.

36. Corten, *Law Against War,* 52-78.

37. See Colonel Gary P. Corn, "Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare,* 62-64 (Oxford University Press, forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071, (arguing for sovereignty as a foundational principle only)[hereinafter Corn, "Cyber National Security"]. For the contrary position arguing that sovereignty is a primary rule of international law, see Michael N. Schmitt & Liis Vihul, "Respect for Sovereignty in Cyberspace," 95 *Texas Law Review* 1639 (2017) [hereinafter, Schmitt & Vihul, "Respect for Sovereignty"]. For this position see also *Tallinn Manual 2.0,* 168-174.

NOTES

38. Speech by Attorney General Jeremy Wright QC, UK, "Cyber and International Law in the 21st Century," May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, [hereinafter *UK AG Speech]; Koh Speech; Egan Speech.*

39. Tom Ruys, "The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded From UN Charter Article 2(4)?" 108 *Am. J. Int'l L.* 159 (2014), (the author "concludes that excluding small-scale or "targeted" forcible acts from the scope of Article 2(4) is conceptually confused, inconsistent with customary practice, and undesirable as a matter of policy.") [hereinafter Ruys, *Meaning of Force*].

40. Corten, *Law Against War,* 52-78; See also *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, (1996) ICJ 14, 246-247, para. 48, (In assessing whether there was a violation of article 2(4), "depends upon whether the particular use of force envisaged would be directed against the territorial integrity or political independence of a State, or against the Purposes of the United Nations or whether, in the event that it were intended as a means of defence, it would necessarily violate the principles of necessity and proportionality."). [hereinafter *Nuclear Weapons*]. See also, A Randelzhofer, "Article 2(4)" in Simma, *The Charter of the United Nations,* 123 ("As the prohibition of the threat or use of force is limited to the international relations between States it is the opinion of various authors that this prohibition does not comprise military acts of protection within the State territory against intruding persons or aircraft.").

41. *Corfu Channel,* 35 ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations . . . [T]he Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty.").

42. Id., 34-35.

43. See Corten, *Law Against War,* 55-67.

44. Id., 52-66.

45. Schmitt, *Peacetime Cyber Responses,* 245 (The *Tallinn Manual 2.0* experts were unable to agree on "when cyber operations not having those consequences [of damage or injury] qualify" as a use of force.). Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998-99), 914-915 [hereinafter Schmitt, "Computer Network Attack"]. The author proposes a list of eight, non-exhaustive factors that states may consider in order to establish when the scale and effects of cyber operations that produce negative effects but non-physical in nature that may resemble that of kinetic uses of force to include, severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality. These factors, as the author admits, are "not legal." See Michael N. Schmitt, "'The Use of Force' in Cyberspace: A Reply to Dr. Ziolkowski," in *2012 4th International Conference on Cyber Conflict* (2012), edited by Christian Czosseck, Rain Ottis and Katharina Ziolkowski, 314. *Tallinn Manual 2.0,* 234-236, 337 (adopting the above factors and the following additional factors for consideration in assessing whether an action constitutes a use of force: "the prevailing political environment, whether the cyber operation portends the future use of military force, the identity of the examiner, and record of cyber operations by the attacker, and the nature of the target."). *Koh Speech.*

46. See *Tallinn Manual 2.0,* 333 (Describing cyber uses of force as "[A]cts that injure or kill persons or physically damage or destroy objects are uses of force."). See also, Schmitt, *Peacetime Cyber Responses* (noting that non-state actors cannot conduct a use of force as meant by article 2(4) of the Charter.)

47. *DoD Law of War Manual,* 998-999 ("Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibition on the resort to force.").

48. Dinstein, "Computer Network Attacks," 103. See Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," 38 *Stanford Journal of International Law* (2002), 207, 209.

49. Roscini, *Cyber Operations,* 46-47. The effects-based approach has been embraced by the United States for cyber operations. *Koh Speech,* 598 ("if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force."). See also, Tallinn Manual 2.0, Rule 69, 330 ("[a]cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."). See Schmitt, "The Law of Cyber Warfare," 269, 281 ("a cyber operation as a use of force . . . causing greater than *de minimis* damage or injury suffices.").

NOTES

50. See *DoD Law of War Manual*, 998-1000 (listing examples of cyber operations that would cross the threshold of a use of force – triggering a nuclear plant meltdown, opening a dam above a populated area and causing destruction; disabling air traffic control services, resulting in airplane crashes and the crippling of a military's logistics systems.).

51. See, e.g., Marco Roscini, "World Wide Warfare – The Jus ad Bellum and the Use of Cyber Force," 14 *Max Planck Yearbook United Nations L.*, (2010), 85.

52. Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, Vol. 6, Issue 3 (2012), 126, 137.

53. See The President's National Infrastructure Advisory Council, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure," *Draft Report*, August 2017, https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf. See also, Daniel R. Coats, Director of National Intelligence, "Statement for the Record, Worldwide Threat Assessment of the Intelligence Community," Senate Select Committee on Intelligence, May 11, 2017, http://www.iranwatch.org/sites/default/files/os-coats-051117.pdf.

54. Schmitt, *Peacetime Cyber Responses*, 246 ("Presumably, states will treat cyber operations with very severe consequences, such as the targeting of the state's economic well-being or its critical infrastructure, as armed attacks to which they are entitled to respond in self-defense. This will likely be the case even when those operations are neither destructive nor injurious.").

55. See Nils Melzer, "Cyberwarfare and International Law," UNIDIR, 2011, 14, arguing that the kinetic equivalence doctrine used to interpret article 2(4), that considers a use of force only those cyber operations that cause material damage comparable to kinetic attacks, is too restrictive. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

56. *Nicaragua,* 1986 ICJ, paras. 118-119, 228.

57. The US has argued that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack" and therefore also a use of force. UN Doc A/66/152, July 15, 2011, 18. In the context of cyber operations, legal scholars have interpreted the threshold of uses of force and armed attacks in cyber to include cyber operations against critical infrastructure with "significant effects" that may not be destructive or injurious. See, Michael Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis," *Lawfare,* January 8, 2015, https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis. Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?," 51, *Naval L. Rev.* 132 (2005), 172. Katharina Ziolkowski, "Computer Network Operations and the Law of Armed Conflict," *Military Law and Law of War Review* 49 (2010), 74-75.

58. See Roscini, *Cyber Operations*, 62.

59. See *Nicaragua*, para. 228, see also Schmitt, "Computer Network Attack," 885.

60. Ian Brownlie, *International Law and the Use of Force by States* 362 (5th ed. 1998). Simma, *Charter of the United Nations*, 208. Schmitt, "Computer Network Attack," 906-908.

61. Dinstein, War, *Aggression and Self-Defence*, 81.

62. See *Nicaragua*, paras. 202, 205; *Corfu Channel*, 35. On intervention in general see Philip Kunig, "Intervention, Prohibition of," *Max Planck Encyclopedia of Public International Law* (2012), Vol. VI, 290. For violations of the norm of non-intervention in the cyber context see *Tallinn Manual 2.0,* 312-325. For violations of the norm of sovereignty or territorial integrity in the cyber context see *Tallinn Manual 2.0*, 17.

63. *Nicaragua*, para. 206.

64. O'Connell, *Use of Force*, 102.

65. Id.

66. Ruys, *Meaning of Force*, (arguing against a minimum threshold for uses of force under article 2(4)). For arguments supporting the position of a minimum threshold for article 2(4) see O'Connell, *Use of Force;* Corten, *The Law Against War*, 77 ("there is a threshold below which the use of force in international relations, while it may be contrary to certain rules of international law, cannot violate article 2(4).").

67. O'Connell, *Use of Force*, 102-107 (while acknowledging that "[t]here is no express authority on the point," the author finds that "Article 2(4) is narrower than it might appear on its face."). See also Robert Kolb, *Ius Contra Bellum* 247 (2d ed. 2009).

NOTES

68. 2 Independent International Fact-Finding Mission on the Conflict in Georgia, *Report* 242 & n. 49 (September 2009), http://www.ceiig.ch/Report.html.

69. Robert Kolb, *International Law on the Maintenance of Peace: Jus Contra Bellum,* (Edward Elgar Publishing, 2018), 337. See also, O'Connell, *Use of Force;* Corten, *The Law Against War,* 55, 77.

70. James Masters, "Theresa May's full statement on Russian spy's poisoning," *CNN.org,* March 13, 2018, https://www.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html.

71. Peter Walker and Andrew Roth, "UK, US, Germany and France unite to condemn spy attack," *The Guardian,* March 15, 2018, https://www.theguardian.com/uk-news/2018/mar/15/salisbury-poisoning-uk-us-germany-and-france-issue-joint-statement.

72. SC Res 138 (1960), June 23, 1960, para. 1; S/PV.865, June 22, 1960, 5, para. 26.

73. Corten, *The Law Against War,* 67.

74. Id. Corten, *The Law Against War,* Id., 55.

75. Roscini, *Cyber Operations,* 54. See *Tallinn Manual 2.0,* 334.

76. See also, 1 Lassa Oppenheim, *Oppenheim's International Law* 432 (Sir Robert Jennings & Sir Arthur Watts, eds., 9th ed. 1992. *Tallinn Manual 2.0,* 213-217.

77. Harold Koh statement on "intent" and "gravity" to assess whether an act is a use of force covered by article 2(4).

78. For a discussion of countermeasures under international law see pages 20-24 and accompanying endnotes.

79. In his separate judgment in *Oil Platforms,* Judge Simma supported the position for defensive actions by force in response to a "smaller-scale use of force." *Oil Platforms,* 332. For views that a right to use force may exist even when an armed attack mentioned in article 51 has neither occurred nor is imminent see Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Collected Courses* (1952–11), 451, 496–497. Thomas Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* (2002), 12 [hereinafter Franck, *Recourse to Force*].

80. For a discussion of the requirements for countermeasures see pages 23-24 and accompanying endnotes.

81. UN Charter, art. 39, 42. See Simma, *The Charter of the United Nations,* 670-671. See Article 3(g), 1975 General Assembly Definition of Aggression, UN GA Res. 3314 (XXIX) 1974.

82. UN Charter, art. 51.

83. Derek W. Bowett, *Self-Defence in International Law* (1958), 188-189. C.H.M. Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Recueil des Cours* (1952 II) (1968), 451, 498 ("[w]here there is convincing evidence not merely of threats and potential danger but of an attack being actually mounted, then an armed attack may be said to have begun to occur, though it has not passed the frontier."). See Dinstein, *War, Aggression and Self-Defence,* 172-173 (discussing anticipatory self-defense as "interceptive self-defense").

84. *Koh Speech*; *UN GGE 2015 Report;* See also *Nicaragua,* paras. 176, 194; *Nuclear Weapons,* 823, paras. 41, 39 (discussing how article 51 applies to "any use of force, regardless of the weapon used"). See also *Tallinn Manual 2.0,* 339.

85. *Nicaragua,* para. 228. For anticipatory self-defense in the cyber context see Terry D. Gill and Paul A.L. Ducheine, "Anticipatory Self-Defense in the Cyber Context," *International Law Studies* 2013. Anticipatory self-defense against imminent cyber armed attacks has been incorporated in Rule 73 of the *Tallinn Manual 2.0,* 350 ("Imminence and immediacy: The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.").

86. See *Tallinn Manual 2.0,* 345 (the majority "concluded that State practice has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, such as terrorist or rebel group."). See also Roscini, *Cyber Operations,* 85 (arguing that the right of self-defense allows states to exercise the right of self-defense against armed attacks by non-state actors, limited by necessity and proportionality).

87. *Nicaragua,* paras. 191,195 (distinguishing between armed attacks and "mere frontier incidents" based on the "scale and effects" of the former.). See Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter* (Cambridge: Cambridge University Press, 2010) ("Scale" refers to the amount of armed force employed or its duration, while "effects" is the damage caused). *Tallinn Manual 2.0* incorporates the scale and effects test for assessing whether cyber operations would constitute uses of force or armed attacks. *Tallinn Manual 2.0,* 330-331, 342.

NOTES

88. Since *Nicaragua*, the US has not recognized any difference between a use of force or an armed attack for purposes of the UN Charter and self-defense, both in kinetic operations and cyber operations. See, e.g., *DoD Law of War Manual*, para. 16.3.3.1 (citing *Koh Speech*). See also, William H. Taft IV, "Self-Defense and the Oil Platforms Decisions," 29 *Yale Journal of International Law* (2004), 295, 299-302.

89. *Koh Speech* ("For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."). *Tallinn Manual 2.0*, para. 8 ("a cyber operation that seriously injures or kills a number of persons or that causes significant damage to or destruction of property would satisfy the scale and effects requirement.").

90. *Oil Platforms*, 72.

91. *Tallinn Manual 2.0*, 342 (reaching no agreement on whether Stuxnet reached the threshold for an "armed attack."). See also, Mary Ellen O'Connell, "Cyber Security without Cyber War," *J. of Con. & Sec. L.*, 17 (2012), 201-202 (arguing that Stuxnet was a violation of the non-intervention norm); Catherine Lotrionte, "Cyber Operations: Conflict Under International Law," *Georgetown Journal of International Affairs*, (2012), 20 (concluding that Stuxnet did not reach the threshold of an "armed attack").

92. *Nicaragua*, para.195. See also, Eritrea-Ethiopia Claims Commission, Jus ad Bellum (Partial Award) 2005, para. 11, http://www.pca-cpa.org/upload/files/FINAL%20ET%20JAB.pdf, ("[l]ocalized border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter.").

93. R. Higgins, *Problems and Process: International Law and How We Use It* (1994), 250-1 (Nicaragua decision may undermine self-defence).

94. *Oil Platforms*, para. 72.

95. Id., 57, 61 (implying that an attack on a single military platform or installation might qualify as an armed attack).

96. Dinstein, "Computer Network Attacks," 105.

97. See *Tallinn Manual 2.0*, 342-343 (concluding that for "cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects" the issue "remains unsettled."). See also, Michael Schmitt, "Cyber Responses 'By The Numbers' in International Law," *EJIL: Talk!*, August 4, 2015, http://www.ejiltalk.org/cyber-responses-by=the-numbers-in-international-law/, (armed attacks can also "include those that seriously impair the functionality of critical infrastructure or that otherwise have devastating non-physical effects, such as crippling a State's economic system . . .") [hereinafter Schmitt, *By The Numbers*].

98. In 2011, the Dutch government endorsed the findings of the report issued by the Dutch Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law. In the context of the threshold for cyber-attacks to constitute an armed attack, the report stated: "A serious, organized cyber-attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. . ." Advisory Council on International Affairs, Cyber Warfare, No. 77, AIV/No. 22, CAVV, (December 2011), 21, http://www.aivadvies.nl/ContentSuite/ upload/aiv/doc/webversie_AIV77CAVV_22_ENG.pdf.

99. Nicholas Tsagourias, "Cyber Attacks, Self-Defense and the Problem of Attribution," *Journal of Conflict and Security Law* 17 (2012), 231 ("a cyber-attack on critical state infrastructure which paralyses or massively disrupts the apparatus of the State should be equated to an armed attack, even if it does not cause immediate human injury or material damage.")[hereinafter Tsagourias, "Cyber Attacks"].

100. Id., 232.

101. James Green, *The International Court of Justice and Self-Defense in International Law* (Oxford: Hart Publishing, 2009), 41.

102. *Nicaragua*, para.231. *Oil Platforms*, para. 64. See also, Tom Ruys, *Armed Attack*, 168.

103. *Tallinn Manual 2.0*, 342. The Group of Experts agreed with the doctrine of "accumulation" when the same state or group of states is responsible for the individual cyber operations at issue.

104. Statement by Dr. Craig Fields, Chairman, Defense Science Board, and Dr. Jim Miller, Member, Defense Science Board and Former Under Secretary of Defense (Policy) Before the Armed Services Committee, "Cyber Deterrence," US Senate, March 2, 2017, https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf, ("[A] **range of state and non-state actors** *have the capacity for persistent cyber-attacks and costly cyber intrusions against the United States, which individually may be inconsequential [or be only one element of a broader campaign] but which cumulatively subject the Nation to a 'death by 1,000 hacks.'*").

NOTES

105. This article does not address the issue of the right of self-defense in cyberspace against non-state actors whose actions are not attributable to a state under international law. On that subject, see *Tallinn Manual 2.0*, 344-346.

106. See *Nuclear Weapons*, para. 41 (quoting *Nicaragua*, para. 176). The requirement of necessity entails determining that there were no other less intensive options than using force in order to stop an ongoing attack or prevent an imminent one from happening. See *Tallinn Manual 2.0*, 348-350 for discussion of the requirement of necessity for cyber operations in the context of self-defense.

107. The requirement of proportionality entails using force in self-defense to the degree it is necessary to eliminate the threat from an armed attack. Dinstein, *War, Aggression and Self-Defence*, 208-12. *Nuclear Weapons*, para. 41 ("[t]he submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law" and "[t]his dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."). As to the requirements of proportionality in the cyber context, see *Tallinn Manual 2.0,* Rules 71-75, 339-356. The US affirmed in a written statement to the UN that a use of force in self-defense against a cyber-attack "must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced." UN Doc. A/66/152, July 15, 2011, 19.

108. Addendum – Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur – the internationally wrongful act of the State, source of international responsibility (part 1), *Yearbook of the International Law Commission*, 1980, vol. II(1), A/CN.4/318/Add.5-7, para. 120 (1980) (According to Ago, "[t]he action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered. What matters in this respect is the result to be achieved by the "defensive" action, and not the forms, substance and strength of the action itself.") [hereinafter Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur].

109. O'Connell, *Power & Purpose,* 172.

110. Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur, para. 120.

111. See *Tallinn Manual 2.0*, 339-356. *UN GGE Report 2015.*

112. See, The United States Diplomatic and Consular Staff in Tehran (*Hostages Case*), Provisional Measures ICJ Reports, 1979, 7, where the ICJ referred to the takeover of the U.S. embassy in Tehran by student protestors as an armed attack. In contrast, see Simma, *The Charter of the United Nations*, 670-671 (Attacks on non-military targets situated outside the territory of the states are not generally regarded as coming within the definition of an armed attack.).

113. *Nuclear Weapons*, para 39 ("any use of force, regardless of the weapons employed" could constitute an armed attack for purposes of Article 51 of the UN Charter.). Karl Zemanek, "Armed Attack," *Max Planck Encyclopedia of Public International Law* (2012), Vol. I, 599. See also *Tallinn Manual 2.0*, Rule 71, para. 4.

114. *Oil Platforms*, para. 72.

115. Dinstein, "Computer Network Attacks," 106-107.

116. *Tallinn Manual 2.0*, 346. In the case of a cyberattack outside the state's territory, against the state's non-governmental facilities, equipment or people, the Group of International Experts for *Tallinn 2.0* could not reach consensus as to the criteria that would be required in order to assess whether such a cyber operation would constitute an armed attack.

117. *Tallinn Manual 2.0*, 349. See, *DoD Law of War Manual*, para. 16.3.3.2.

118. See *UN GGE Report 2015*, para. 28(f). In the section of the report on the "application of international law" it notes that "accusations of organizing and implementing wrongful acts brought against States should be substantiated." No further details were included regarding any agreement about what kind of, or how much, evidence would be required. In an attempt to potentially develop a new rule of international law requiring a state to publicly disclose information that was the basis of its attribution assessment of illegal cyber operations of another state, the Russians insisted this language be added to the *UN GGE 2015 Report*.

119. See Ian Brownlie, *International Law and the Use of Force by States* 21, (1963), 220.

120. B.O. Bryde, "Self-Help," in *Encyclopedia of Public International Law*, Vol. 4, (1982), 213-15. See also R.A. Falk, "The Beirut Raid and the International Law of Retaliation," 63 *Am. J. of Int'l L.* (1969) 429, ("at present, international society is not sufficiently organized to eliminate forcible self-help in either its sanctioning or deterrent roles.").

NOTES

121. Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S Cyber Command and Director, National Security Agency/Chief, Central Security Service, 27, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf.

122. See International Law Commission, Responsibility of States for Internationally Wrongful Acts, GA Res 56/83 annex, UN Doc. A/RES/56/83, December 12, 2001, art. 50(1)(a), [hereinafter *Articles of State Responsibility*]. See *Oil Platforms*, Judge Simma's separate opinion supported forcible proportionate countermeasures in response to a "smaller-scale use of force." *Oil Platforms*, para. 12, 332. For views that a right to use force may exist even when an armed attack mentioned in article 51 has neither occurred nor is imminent see Waldock, "The Regulation of the Use of Force by Individual States in International Law," 81 *Collected Courses* (1952–11) 451, 496–497. Franck, *Recourse to Force,* 12. See *Tallinn Manual 2.0*, 330.

123. *Tallinn Manual 2.0*, 79, describing how the Rules are based on the *Articles of State Responsibility*. For information on the International Law Commission's work, see http://www.un.org/law/ilc/index.htm.

124. *Articles of State Responsibility*, arts. 20-26 (listing six circumstances precluding the wrongfulness of conduct that would otherwise constitute a breach of an international obligation of the state concerned: consent, self-defense, countermeasures, necessity, *force majeure*, and distress.).

125. See *Articles of State Responsibility*, art. 1. See also James Crawford, *State Responsibility: The General Part* 43 (Cambridge University Press, 2013), (The *Articles of State Responsibility* "are considered by courts and commentators to be in whole or in part an accurate codification of the customary international law of state responsibility."). *Tallinn Manual 2.0,* at n. 112, 79.

126. See endnote 138 and accompanying text.

127. See Oscar Schachter, *International Law in Theory and Practice* (1995), 184-186. With the new prohibition on armed force for enforcement purposes in the UN Charter, reprisals were replaced with the term "peaceful reprisals" or coercive measures that were forcible but not in violation of article 2(4) of the UN Charter. The term countermeasures evolved to replace the term peaceful reprisal. Over time, international tribunals and the ILC determined that such actions could not be taken against the state conducting the wrongful act as a matter of punishment or revenge but only to induce that state to comply with its legal obligations. See *Articles of State Responsibility*, art. 49. See *Air Services Agreement of 27 March 1946* (US v. France), 18 RIAA 416 (1979), 54 ILR 337, 444 (in replacing the term peaceful reprisals with "countermeasures," ruled they were "contrary to international law but justified by a violation of international law allegedly committed by the State against which they are directed …") [hereinafter *Air Services*] . See also, *Gabčíkovo -Nagymaros Project* (Hungary v. Slovakia), (1997) ICJ 7 (September 27), paras. 82, 55. [hereinafter *Gabčíkovo –Nagymaros*].

128. *Articles of State Responsibility*, chapeau to Chapter II of Part 3, para. 3. *Egan Speech* ("a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States. Such acts—which are known as acts of retorsion—may include, for example, the imposition of sanctions or the declaration that a diplomat is persona non grata.").

129. Id. *Articles of State Responsibility*. See also James Crawford, *Fourth Report,* para. 35, UN Doc. A/ CN.4/517 and Add. 1 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf. *Tallinn Manual 2.0*, Rule 20, para.4.

130. There is often some confusion on the distinction between retorsions and countermeasures. Indeed, it is often difficult to draw a distinction between a retorsion and a countermeasure when discussing "sanctions." In a general sense, countermeasures and retorsions are sanctions in that a state is seeking to exercise pressure on another state through the use of sanctions. However, sanctions are mere "unfriendly acts" (retorsions) and are always allowable when they do not imply any violation of international obligations. However, in cases where sanctions do violate an international obligation owed to a state, such sanctions would constitute countermeasures. In short, indictments and sanctions (unless unlawful) are not considered countermeasures as a legal matter. These examples would be retorsions. See, Article 30 of the *Articles of State Responsibility* Provisionally Adopted by the International Law Commission on First Reading (1996), reproduced in Report of the International Law Commission on the Work of its Forty-Eighth Session, UN Doc. A/51/10, 125.

131. Dan Roberts, "Obama Imposes New Sanctions Against North Korea in Response to Sony Hack," *The Guardian*, January 2, 2015, http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-theinterview.

NOTES

132. Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

133. Evan Perez and Daniella Diaz, *CNN*, "White House Announces Retaliation Against Russia: Sanction, ejecting diplomats," January 2, 2017, http://www.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-whitehouse/. See also, The White House, *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*, December 29, 2016, https://obamawhitehouse.archive.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and. Mark Mazzetti and Adam Goldman, "The Game Will Go On as U.S. Expels Russian Diplomats," *The New York Times*, December 30, 2016, https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html?_r=.

134. Beyond carrying out retorsions, because of the nature of the actions by North Korea and Russia were illegal under international law, the US could have also conducted countermeasures against North Korea and Russia. For an analysis of the DNC hack and possible legal responses under international law see Sean Watts, "International Law and Proposed U.S. Responses to the D.N.C. Hack," *Just Security*, October 14, 2016, https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/. For legal analysis of the Sony hack see Michael N. Schmitt, "International Law and Cyber Attacks: Sony v. North Korea," *Just Security*, December 17, 2014 (arguing that while the Sony hack most likely would not be considered a use of force or intervention under international law it was a violation of US sovereignty.), http://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea.

135. *Tallinn Manual 2.0*, 112. (In giving an example of a lawful retorsion, "A State may, for instance, employ an access control list to prevent communications from another State because the former enjoys sovereignty over the cyber infrastructure on its territory."). However, the Group of Experts of *Tallinn Manual 2.0* agreed "[A] receiving State may not suspend international cyber communication services upon which a diplomatic mission or consular post relies because according to Rule 42 [of *Tallinn Manual 2.0*] it must permit the mission or post's free electronic communications." *Tallinn Manual 2.0*, 294. See also ITU Constitution, arts. 34(2) and 35, specifying the conditions for a state's right to interrupt the flow of telecommunications.

136. *Articles of State Responsibility*, arts. 48, 54. See also *Tallinn Manual 2.0*, 111. Only one state, Mexico, opposed the inclusion of countermeasures in the *Articles of State Responsibility*, arguing that they "[do] not seem to accord with internationally recognized principles on the peaceful coexistence of States." Comments and Observations received by governments, A/CN.4/488, March 25, 1998, 83.

137. See *Air Services*, para. 81 ("Under the rules of present-day international law, and unless the contrary results from special obligations arising under particular treaties . . . [a] State is entitled . . . to affirm its rights through 'countermeasures'."). *Nicaragua*, 14, 127, para. 248. Reparations may include restitution, compensation, and satisfaction. *Articles of State Responsibility*, arts. 34-37. On reparations for cyber operations see *Tallinn Manual 2.0*, Rule 29.

138. During the drafting the *Articles of State Responsibility*, the US stated "[w]hile we welcome the recognition that countermeasures play an important role in the regime of state responsibility, we believe that the draft articles contain unsupported restrictions on their use." *United States: Comments on the Draft Articles on State Responsibility*, 37 ILM 468 (1998). For an analysis of the US' specific objections on the draft articles, including on countermeasures, see Sean Murphy, "U.S. Comments on ILC Draft Articles of State Responsibility," 3 *Am. J. of Int'l L.* 95, (July 2001), 626-628 (related to countermeasures US objections included the list of restrictions in articles 50-55, the use of the word "commensurate" instead of "proportionate," and the use of the words "rights in question" without further elaboration.) [hereinafter Murphy, "US Comments on ILC Draft Articles"]. For a list of the requirements for countermeasures in the Articles see, A list of requirements for countermeasures in the *Articles of State Responsibility* includes: a prior wrong suffered, prior notice to an offending state before commencing countermeasures, proportionality, measures shall not amount to a use of force as meant by art. 2(4) of the Charter, shall not violate human rights, shall not constitute reprisals or violate jus cogens norms, its purpose must only be to induce compliance or reparation, offer of negotiation must be occur before countermeasures are taken, and must conclude when the offending state has complied with its obligations. *Articles of State Responsibility*, arts. 22, 30-31, 33-37, 42, 48(1), 50-54. *Tallinn Manual 2.0*, Rules 20-25. See also, *Gabčíkovo –Nagymaros*. In the context of whether countermeasures can violate art. 2(4) see, *Articles of State Responsibility*, arts. 22, 52, 51, 50(1), and 52 respectively. *Tallinn Manual 2.0*, Rule 22, para. 10 ("[the experts] were divided over whether cyber countermeasures crossing the use of force threshold, but not reaching that of an armed attack, are lawful.").

NOTES

139. The reasons the UN GGE failed to reach agreement on a final report in 2017 included disagreements among states as to whether countermeasures were applicable to cyber operations as well as the right of self-defense. See Michael Schmitt & Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," *JustSecurity.org*, June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/. See also, *UK AG Speech* (disagreeing with the Articles of State Responsibilities' stating that a state is not "always legally obliged to give prior notification to the hostile state before taking countermeasures against it.")

140. *Articles of State Responsibility*, art. 51 ("Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."). The US had objected to the use of the word "commensurate" instead of "proportionate" since it could be misinterpreted to mean something narrower then proportionate which would not be in accord with state practice. See, Murphy, "US Comments on ILC Draft Articles," 628. See also Lori Fisler Damrosch, "Retaliation or Arbitration – Or Both? The 1978 United States-France Aviation Dispute," 74 Am. J. of Int'l L. 4, (1980), 785, 792 (In analyzing the ICJ *Air Services* decision on the proportionality of countermeasures, "it permits states to apply countermeasures that would be disproportionate in an economic sense, in order to enforce a principle.") [hereinafter Damrosch, "Retaliation or Arbitration."]. See *Tallinn Manual 2.0*, 127.

141. See *Yearbook of the ILC, 2001*, Vol. 11 (2), 135 citing to para. 7 of the commentary to art. 51 of the Article of State Responsibility ("[A] clearly disproportionate measure may well be judged not to have been necessary to induce the responsible State to comply with its obligations but to have had a punitive aim and to fall outside the purpose of countermeasures enunciated in article 49."). See *Gabčíkovo –Nagymaros*, 55. *Air Services*, paras. 80-98. See also, *Egan Speech* ("[U]nder the law of countermeasures, measures undertaken in response to an internationally wrongful act performed in or through cyberspace that is attributable to a State must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality. . .").

142. The ICJ in *Nicaragua* cast doubt on the right of states to participate in collective countermeasures as it ruled that only the target of the unlawful intervention may legally respond. *Nicaragua*, para. 211, 110-111. See also, James Crawford, *The International Law Commission's Articles of State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002), 305 (arguing that existing state practice is scarce and mainly limited to Western states therefore the law is uncertain today) [hereinafter Crawford, *ILC's Articles of State Responsibility*]. In contrast see, L. A. Sicilianos, "Countermeasures in Response to Grave Violations of Obligations Owed to the International Community," in Crawford, Pellet and Olleson (eds.), *The Law of International Responsibility* (Oxford University Press, 2010), 1137 (arguing there is sufficient practice to support the view that states can take countermeasures against third states when they violate obligations owed to the international community).

143. *Articles of State Responsibility*, art. 54, paras 6-7 of the ILC's commentary. See *Case Concerning Barcelona Traction, Light & Power Company Limited* (Spain v. Belgium) February 5, 1970, ICJ Reports 1970, para. 33, 33 (observing that obligations *erga omnes* are the "concern of all States" and "owed towards the international community as a whole"; that "all States . . . have a legal interest in their protection."). For a detailed discussion on erga omnes obligations and their impact on standing and countermeasure responses in international law see Christian J. Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge: Cambridge University Press, 2005), 231 ("at least in the case of systemic or large-scale breaches of international law . . . a settled practice [exists] of countermeasures by states not individually injured."). *Tallinn Manual 2.0*, 132 ("[The majority of experts concluded] that States may not lawfully take countermeasures on behalf of another State. . .").

144. In identifying the limitations for cyber countermeasures, the *Tallinn Manual 2.0* experts were unable to agree on whether such countermeasures that triggered the article 2(4) threshold of a use of force would be lawful, *Tallinn Manual 2.0*, 125. See *Articles of State Responsibility*, art. 50(1)(a), 131 ("Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations").

145. *Tallinn Manual 2.0*, Rule 22, para. 14 ("all of the Experts agreed that cyber countermeasures might not rise to the level of an armed attack"), 126. However, because the experts could not agree on whether a forcible cyber countermeasure that was not of the intensity of an armed attack would be lawful, there was "no limitation" on forcible countermeasures included in Rule 22 on countermeasures in the *Tallinn Manual 2.0*. See *Tallinn Manual 2.0*, Rule 22, paras. 10-12 ("A minority of the Experts asserted that forcible countermeasures are appropriate in response to a wrongful use of force that itself does not

NOTES

(145. *cont.*) qualify as an armed attack . . . "), 125-126. See also, *Oil Platforms* and Judge Simma's dissenting opinion supporting a state's limited right to undertake proportionate countermeasures involving the use of force when confronted with "smaller-scale use of force," not amounting to an "armed attack." *Oil Platforms*, para. 12, 331 (separate opinion of Judge Simma). But see *Articles of State Responsibility*, art 50(1)(a), 57 ("[c]ountermeasures shall not affect . . . the obligations to refrain from the threat or use of force as embodied in the Charter of the United Nations.").

146. Tom Ruys, *Armed Attack*, 141.

147. *Articles of State Responsibility*, Art. 50(1)(a)("1. Countermeasures shall not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations")

148. *Tallinn Manual 2.0*, Rule 22, para. 10, 125.

149. Judge Abdulqawi A. Yusuf, Symposium: The Nicaragua Case 25 Years Later, "The Notion of 'Armed Attack' in the Nicaragua Judgment and Its Influence on Subsequent Case Law," 25 *Leiden Journal of International Law* (2012), 461-470, 466.

150. Mary Ellen O'Connell, "The True Meaning of Force," *AJIL Unbound*, August 4, 2014, https://www.asil.org/blogs/true-meaning-force. Judge Simma, *Oil Platforms*, dissenting opinion.

151. *Tallinn Manual 2.0*, 111 ("A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State.").

152. O'Connell, *Power & Purpose*, 248. See also Oscar Schachter, *International Law in Theory and Practice* 187 (1995); Damrosch, "Retaliation or Arbitration," 795 ("It seems preferable to adopt a rule allowing a state to implement countermeasures without risk of later liability when it acts upon a good faith belief that it is the victim of a breach, even though that belief turns out to be erroneous . . ."). See also *Egan Speech*, 17 ("[I]nternational law generally requires [only] that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.").

153. For a review of state practice in cases of military uses of force made in error see, Corten, *Law Against War*, 79-81; Air Services, paras. 74, 77-78, 83, 90-98; Appellate Body Report, *United States – Importation Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/RW (Oct. 22, 2001) (The US was found to be using countermeasures inconsistent with GATT obligations but no responsibility was found for such measures).

154. See *Tallinn Manual 2.0*, Rule 20, para. 16 ("States taking countermeasures do so at their own risk"). *Articles of State Responsibility*, 301-310 ("A State that resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment."). See also, James Crawford, Special Rapporteur of the International Law Commission, *Third Report on State Responsibility*, para. 294, 79, UN Doc. A/CN.4/507/Add.3 ("Countermeasures can only be taken in response to conduct actually unlawful; and a "good faith belief" in its unlawfulness is not enough."). The *Articles of State Responsibility* and the *Tallinn Manual 2.0* allow mistake for self-defense actions but not for countermeasures. See *Tallinn Manual 2.0*, Rule 71, para. 14 ("the lawfulness of the response would be determined by the reasonableness of the State's assessment as to whether an armed attack was underway against it."). It would seem that given the general reversibility of countermeasures, making the harm only temporary, the argument for mistake for countermeasures would seem even stronger more so than with acts of self-defense which can be deadly and non-reversible.

155. *Gabčíkovo –Nagymaros*, paras. 82-87 (setting down four elements of a lawful countermeasure: 1) it must be taken in response to a prior wrongful international act, 2) the injured state must call on the state conducting the wrongful act to stop or to make reparations, 3) the effects of the countermeasures must be commensurate with the injury suffered, and 4) the purpose must be to induce the other state to comply with its legal obligations.). For a discussion of the list of restrictions on countermeasures in the cyber context see Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," 54 *Virginia Journal of International Law* 3, 697-732 (2014) [hereinafter Schmitt, *Countermeasures*]. Under Article 50(1) of the *Articles of State Responsibility*, another requirement is that certain obligations cannot be affected by countermeasures, to include obligations related to the protection of human rights (art. 50(1)(b)) and obligations related to the inviolability of diplomatic or consular agents, premises, archives and documents (art. 50(2)(b)) and other preemptory norms.

NOTES

156. Schmitt, *Countermeasures* ("countermeasures are reactive, not prospective"). See also, *Gabčíkovo –Nagymaros*, para. 83 (Countermeasures "must be taken in response to a previous international wrongful act of another State."), 715.

157. *Articles of State Responsibility* at art. 49(1), 52(1). *Gabčíkovo –Nagymaros*, para. 82-83. *Tallinn Manual 2.0*, 120 ("the notification requirement is not categorical . . . it may be necessary for an injured State to act immediately in order to preserve its rights and avoid further injury.").

158. *UK AG Speech* (In describing one aspect that the UK government disagrees with the ILC about countermeasures, "we would not agree that we are always legally required to give prior notification to the hostile state before taking countermeasures against it.").

159. *Tallinn Manual 2.0*, 120 (concluding that notice was not required if doing so would render it countermeasures ineffective.).

160. *Articles of State Responsibility*, Art. 49(1), 49(3). *Gabčíkovo –Nagymaros*, para. 87, 56-57. For reversibility considerations in the cyber context see *Tallinn Manual 2.0*, Rule 21, para. 8 ("[T]he requirement of reversibility is broad and not absolute"), 119.

161. *Articles of State Responsibility*, art 22, para. 5. See also, Schmitt, *Countermeasures*, 728-729.

162. Schmitt, *Peacetime Cyber Responses*, 258 ("countermeasures need not be in-kind nor directed at the entity that authored the internationally wrongful act").

163. *Tallinn Manual 2.0*, 133.

164. Schmitt, *Countermeasures*, 717.

165. Corten, *The Law Against War*, 55-66.

166. *Articles of State Responsibility*, ch. V, art. 25. *Tallinn Manual 2.0*, 135.

167. See *Russian Indemnity* (Russia v. Turkey), November 11, 1912, 12 RIAA 44; *Gabčíkovo –Nagymaros*, 7; *M/V SAIGA* (No. 2), (Saint Vincent and the Grenadines v. Guinea), International Tribunal for the Law of the Sea (1999), 38 ILM 1323.

168. *Articles of State Responsibility*, art. 25 (stating that necessity may negate state responsibility if the act "(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."). See also *Gabcíkovo –Nagymaros*, paras. 51, 52 ("the state of necessity is a ground recognized by customary international law for precluding the wrongfulness of an act not in conformity with an international obligation."). *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J., 136, ¶ 140 (July 9) (In applying the defense of necessity under customary law, the ICJ notes that it only applied in "strictly defined conditions."). The arbitral tribunal constituted to hear the Sempra Energy International v Argentine Republic case, in its 2007 award, considered the customary international law status of article 25 of the State responsibility articles on Necessity and concluded that art. 25 reflected customary international law on the issue, stating, "This not to say that the Articles are a treaty or even themselves a part of customary law. They are simply the learned and systematic expression of the law on state of necessity developed by courts, tribunals and other sources over a long period of time." ICSID, *Sempra Energy International v Argentine Republic*, Case No ARB/02/16, award, September 28, 2007, para 244.

169. Jens David Ohlin and Larry May, *Necessity in International Law* (Oxford University Press, 2016), 39.

170. *Yearbook of the ILC,* Report of the International Law Commission on the work of its fifty-third session, A/CN.4/SER.A/2001/Add.1 (Part 2), art. 25, at 80, para. 14 of commentary, http://legal.un.org/ilc/publications/yearbooks/english/ilc_2001_v2_p2.pdf.

171. On this point, the final version of the *Articles of State Responsibility* were silent noting that it was an issue to be dealt in accordance with a review of the relevant primary rules, such as article 2(4) of the Charter. See *Articles of State Responsibility*, Commentary to art. 25, para. 21. The Tallinn Manual experts were unable to reach a conclusion on the issue. *Tallinn Manual 2.0,* Rule 26, para. 18, 140. See Report of the ILC, 32nd Session, *ILC Yearbook 1980*, Vol. II (1), 1, 43, para. 23 ("certain actions by States in the territory of other States which, although they may sometimes be of a coercive nature, serve only limited intentions and purposes bearing no relation to the purposes characteristic of a true act of aggression.").

172. *Articles of State Responsibility*, art. 25.

NOTES

173. *Gabčíkovo –Nagymaros*, para. 53, 7, 41. R Ago, Addendum to the Eighth Report on State Responsibility, *ILC Yearbook 1980*, Vol. II(1), para. 78, 13, 50.

174. *Articles of State Responsibility*, Commentary to art. 25, para. 16.

175. *Articles of State Responsibility*, art, 25(1)(a). See also, Roberto Ago, "Addendum to the Eighth Report on State Responsibility" (1980, vol. II), *Yearbook of the International Law Commission* 15, 19 (In assessing how "essential" a given interest of a state must be, "it naturally depends on the totality of the conditions in which a State finds itself in a variety of specific situations: it should, therefore, be appraised in relation to the particular case in which such an interest is involved, and not predetermined in the abstract."). Examples of "essential interests" that have been suggested include the political or economic survival of the state, the continuous functioning of essential services, the survival of a sector of the population, and the preservation of the environment. See Addendum to Eighth Report, on State Responsibility by Mr. Roberto Ago, (1980) 2 *Yearbook of International Law*, Commentary 51, para. 12, UN Doc A/CN.4/318/ADD.5-7. *Tallinn Manual, 2.0*, 135.

176. *Articles of State Responsibility*, art. 25 (1)(b). *Tallinn Manual 2.0*, 137.

177. *Tallinn Manual 2.0*, 137.

178. *Articles of State Responsibility*, Commentary to art. 25, para. 16 ("the peril is clearly established on the basis of the evidence reasonably available at the time.").

179. Crawford, *ILC's Articles of State Responsibility*, para. 17, 184; *Articles of State Responsibility*, Commentary to art. 25, para. 20. *Tallinn Manual 2.0*, 140.

180. Schmitt, *By The Numbers.* See also, *Tallinn Manual 2.0,* 138 ("[I]f significant cyber operations of unknown origin target its critical infrastructure, the plea of necessity could justify a State's resort to counter-hacking."). On the requirement of imminence, a rule of reason applies. *Tallinn Manual 2.0*, 138 ("This standard allows some degree of uncertainty as to whether the offending operation will occur, whether sufficient harm will ensue to justify a plea of necessity and the identity of the originator of the operation.").

181. *Tallinn Manual 2.0,* 136-137 (examples of situations that gravely threaten the essential interests of a state through cyber operations that are provided include: cyber operations that would debilitate the State's banking system, cause a dramatic loss of confidence in its stock market, ground planes nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records, cause a major environmental disaster, among others.).

182. See Corn, "Cyber National Security" (arguing for sovereignty as a foundational principle only); Schmitt & Vihul, "Respect for Sovereignty in Cyberspace" (arguing for sovereignty as a primary rule of international law). See also, *UK AG Speech* ("Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention."); *Egan Speech* ("[P]recisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and *opinio juris.*").

183. Hugo Grotius, *The Law of War and Peace in Three Books* (Francis W, Kelsey tr, 1625) book III, ch. XXI, section.

184. U.S., *National Security Strategy*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

185. Speech by Secretary of State for Defence, UK, "Defence Secretary's speech to RUSI on the SDSR 2015," September 22, 2015, https://www.gov.uk/government/speeches/defence-secretarys-speech-to-rusi-on-the-sdsr-2015.

186. See, e.g., *UK AG Speech.*

187. For deterrence in cyberspace, see Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence Report,* February 2017; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," 41 *International Security* 44 (Winter 2016/17); Catherine Lotrionte, "Cyberwar: Building a Normative and Legal-Based Approach for Cyberdeterrence," in *Law and Disciplinarity: Thinking Beyond Borders,* (Palgrave Macmillan US, 2003), 67-99.

Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems

Martin "Trae" Span
Logan O. Mailloux
Michael R. Grimaila

ABSTRACT

In the modern military's highly interconnected and technology-reliant operational environment, cybersecurity is rapidly growing in importance. Moreover, as a number of highly publicized attacks have occurred against complex cyber-physical systems such as automobiles and airplanes, cybersecurity is no longer limited to traditional computer systems and IT networks. While architectural analysis approaches are critical to improving cybersecurity, these approaches are often poorly understood and applied in ad hoc fashion. This work addresses these gaps by answering the questions: *1. "What is cybersecurity architectural analysis?"* and *2. "How can architectural analysis be used to more effectively support cybersecurity decision making for complex cyber-physical systems?"* First, a readily understandable description of key architectural concepts and definitions is provided which culminates in a working definition of "cybersecurity architectural analysis," since none is available in the literature. Next, we survey several architectural analysis approaches to provide the reader with an understanding of the various approaches being used across government and industry. Based on our proposed definition, the previously introduced key concepts, and our survey results, we establish desirable characteristics for evaluating cybersecurity architectural analysis approaches. Lastly, each of the surveyed approaches is assessed against the characteristics and areas of future work are identified.

Keywords—cybersecurity; architectural analysis; system architecture; systems security engineering; complex system security

MARTIN "TRAE" SPAN III is an Instructor of Systems Engineering at the United States Air Force Academy (USAFA), Colorado Springs, Colorado. He is commissioned as Captain in the United States Air Force (USAF). He received his undergraduate degree in Systems Engineering in 2012 from USAFA and is a recent distinguished graduate from the Air Force Institute of Technology (AFIT) with a Master of Science in Systems Engineering. He serves as a developmental engineer and holds Department of Defense certifications in systems engineering, science and technology management, test & evaluation, and program management. He has served the USAF as a developmental test engineer responsible for planning and executing complex weapon system test and evaluation. He is a member of IEEE and the Tau Beta Pi Honor Society. Capt. Span's research interests include systems engineering and systems security engineering. He can be contacted at: martin.span.1@us.af.mil

I. INTRODUCTION

The cybersecurity threat is one of the most serious economic and national challenges we face as a nation—economic prosperity in the 21st century depends on cyber [1]. Cyberattacks have grown in frequency and complexity, and it is now commonplace to hear of widespread cyberattacks on personal computers, webservers, and even large company and government personnel databases [2]. Moreover, as the Internet of Things (IoT) continues to grow, the centrality of cyber-physical devices to modern life is increasingly important [3]. Previously, cyber-physical systems such as automobiles and airplanes were relatively simplistic. Astonishingly, the 2017 Ford F-150, a relatively common vehicle, has over 150 million lines of code [4], demonstrating the complexity of modern systems when software is at the core of functionality [3]. For these cyber-enabled systems, adversaries are challenging traditional assumptions that systems are secure due to their relative isolation and uniqueness. Recent examples include a widely-publicized hacking demonstration against a Jeep Cherokee [6]. claims of hacking a commercial airliner [7], and comprehensive reports of vehicle vulnerabilities [3]. In light of this growing threat, it is critical to analyze modern weapon systems for cybersecurity vulnerabilities as directed by the United States Congress to mobilize industry to counter these attacks [9].

Recent Department of Defense (DoD) policy updates have expanded the traditional IT security approaches and mandated cybersecurity assessments for cyber-enabled weapon systems [9], [10], [11], [12]. These revisions dictate that acquisition programs integrate cybersecurity efforts into existing systems engineering processes, and work to ensure

LOGAN O. MAILLOUX (BS 2002, MS 2008, Ph.D. 2015) is an Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio USA. He is commissioned as Lieutenant Colonel in the United States Air Force (USAF) and serves as a computer developmental engineer. He is a Certified Information System Security Professional (CISSP), Certified Systems Engineering Professional (CSEP), and holds Department of Defense certifications in cyberspace operations, systems engineering science and technology management, T&E, and program management. He is a member of IEEE, INCOSE, and ITEA professional societies, as well as, HKN and TBP honor societies. He has served the USAF as a cyberspace operations expert responsible network defense exercises, documenting and training computer security best practices and performing T&E of enterprise resource planning solutions. Lt Col Mailloux's research interests include systems security engineering, quantum key distribution, cyber-physical systems, and complex information systems. He can be contacted at: Logan.Mailloux@us.af.mil

cyber considerations hold equal footing with other requirements and design trade-offs at major acquisition milestones [13].

For highly complex systems, including DoD weapon systems, architectural analysis is a critical enabler to effective cybersecurity; however, architectural analysis approaches are often poorly understood and applied in ad hoc fashion. This work addresses these gaps by answering the questions:

1. *"What is cybersecurity architectural analysis?"*
2. *"How can architectural analysis be used to more effectively support cybersecurity decision making for cyber-physical systems?"*

This paper examines and proposes answers to the above questions. In Section II, we provide a readily understandable discussion of key concepts and definitions. Section III expands on this foundation and surveys several cybersecurity architecture analysis approaches from government and industry. In Section IV, desirable characteristics for architectural analysis for cybersecurity are identified and mapped to the approaches from Section III. Lastly, Section V summarizes key findings and identifies promising follow-on research areas for increasing the effectiveness of cybersecurity architectural analysis of unprecedented systems, specifically modern complex cyber physical systems.

II. FOUNDATIONAL CONCEPTS AND DEFINITIONS

This section provides a brief historical context for system-level architectural analysis and, more formally, discusses key definitions for cybersecurity architectural analysis.

A. Brief History of System Architecture

Much of the seminal work in the field of architecture analysis was accomplished by Zachman, who proposed the first system architecture—a logical

MICHAEL R. GRIMAILA, PhD, CISM, CISSP (BS 1993, MS 1995, PhD 1999) is Professor and Head of the Systems Engineering and Management department at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. Dr. Grimaila holds the Certified Information Security Manager (CISM), the Certified Information Systems Security Professional (CISSP), and the National Security Agency's INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM) certifications. Dr. Grimaila is a Fellow of the Information Systems Security Association (ISSA), a Senior Member of the Institute for Electrical and Electronics Engineers (IEEE), and is a member of the Association for Computing Machinery (ACM), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2), Eta Kappa Nu, and Tau Beta Pi. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management, and systems engineering. He can be contacted at Michael.Grimaila@afit.edu.

construct for integrating the complexities of modern information systems [14]. Similarly to the varying levels of abstraction in physical construction plans, Zachman argued that system architectures should be composed of many perspectives in varying levels of detail. Moreover, he insisted that these perspectives (or views) be synchronized across the system, forming one integrated architecture.

Sowa expanded Zachman's work to form the Information Systems Architecture (ISA) framework [15]. Shown in Fig. 1, the ISA employs six interrogatives (what, how, where, who, when, and why) across five levels of detail (scope, business, system, technology, and detailed representations) as a means of expressing relationships to guide complex system development [16]. In this way, the ISA offers a simplified approach to compare and elaborate on the desired capabilities, requirements, components, and functions in an integrated enterprise-level model which enables effective decision making. Note, not all 30 conceptual graphs are required; thus, the ISA is also tailorable. Since its inception, the ISA (commonly known as the Zachman Framework) has been a popular choice for system architects—it has been widely used by system architects for decades, while several other system-level frameworks have incorporated or adopted its tenets [17].

B. Key Definitions

Here we discuss definitions for key terminology used in this work (i.e., "cybersecurity," "architecture," and "analysis"). First, the term "cybersecurity" should be addressed because it is generally the most poorly understood (see sidebar in [16]). Within the DoD, cybersecurity is formally defined as:

> The prevention of damage to, protection of, and restoration of electronic systems to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [19].

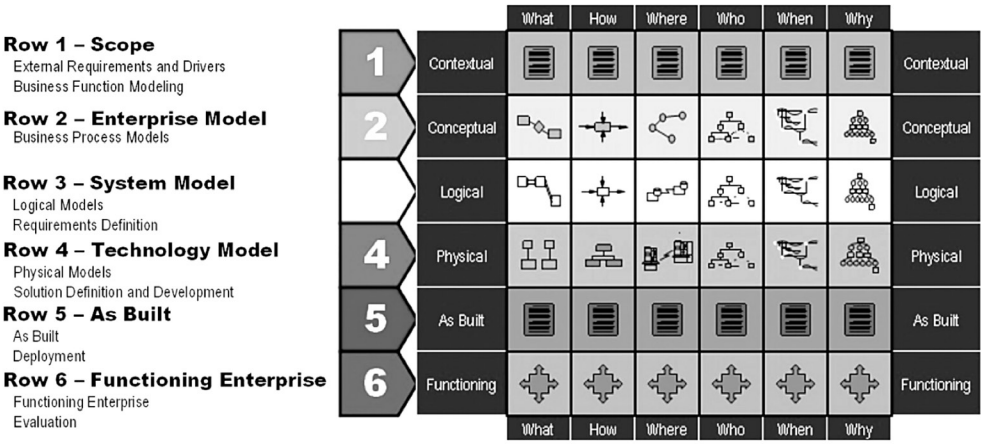


Figure 1. The Zachman Framework for Enterprise Architecture [24].

Despite being often cited, this definition tends to cause confusion because it is packed with domain-specific IT jargon: availability ensures the system is usable as anticipated; integrity is the protection from unauthorized modification; confidentiality is keeping data private; authentication is a validation of the claimed identity; and, nonrepudiation is the ability to prove that an action has taken place. While seemingly comprehensive, the DoD definition is somewhat hindered with legacy terminology; a more practical (i.e., a working) definition of cybersecurity might simply seek to protect critical systems against cyber-based threats [20].

The next key term to define is "architecture" (note, we interpret "architecture" synonymously with "system architecture" and/or "system-level architecture"). Perhaps the most classically understood definition of architecture is provided by Maier and Rechtin:

> Structure in terms of components, connections, and constraints of a product, process, or element [21].

This definition offers a holistic view of the system of interest to include technological aspects as well as non-technological aspects, such as processes. In the simplest terms, an architecture merely provides a means for viewing the system of interest from different perspectives. Conversely, in a somewhat physically-driven characterization, ISO/IEC/IEEE 42010 provides the following definition for architecture:

> The fundamental organization of a system, embodied in its components, their relationship to each other and the environment, and the principles governing its design and evolution [22].

Somewhat surprisingly, the DoD provides a progressive definition of system architecture:

> A set of abstractions (or models) that simplify and communicate complex structures, processes, rules, and constraints to improve understanding and implementation [23].

In addition to being readily understandable, this definition alerts the reader to the intrinsic value offered by such architectures in that they serve to simplify communication with, and improve understanding of, key stakeholders (not just engineers). Moreover, this definition implies that architectures are intended to improve the system's implementation. While these value-rich aspects of the definition are a bit atypical, they are useful for helping others to understand what an architecture is and does.

Lastly, the task of identifying a formal definition of "analysis" within the context of a "system architecture" proved more difficult than previous definitions. Often a systems architecture will center on an integrated model of entities and the relationships between them; architectural models serve as a vehicle to bring order, and thus understandability, to the growing complexity associated with complex systems. An architecture-focused definition may read as such:

> Architectural analysis is the activity of discovering important system properties using conceptual and physical models of the system of interest [25].

However, an architecture's purpose is to increase understanding and facilitate better engineering choice [17]. This two-fold purpose is acutely stated by Crawley *et al.*:

> Architectural analysis focuses on understanding both the architecture's function and form to support decision making [26].

It is worth noting the closely related concept of architecture trade-off analysis, which focuses on evaluating and comparing alternative architecture-level designs and attributes (e.g., modifiability, security, performance, reliability, etc. [27].

C. Cybersecurity Architectural Analysis Working Definition

Ultimately, architectural analysis identifies trade-off points among system attributes and facilitates communication among stakeholders (e.g., customers, developers, operators, maintainers). System-level architectural analysis requires consideration of various missions, essential functions, potential components, and desirable attributes, which help to clarify and refine stakeholder needs and, later, requirements. Moreover, integrated architectural analysis provides a robust framework for ongoing and concurrent system design and analysis.

Specific to the cyber domain, architectural analysis should be used to understand cyber dependencies within the functions and form of the system to enable well-informed decisions. This type of structured analysis brings an otherwise unmanageable amount of information under control in support of system security requirements [28]. Architectural

analysis enables system-level programmatic risk management by providing context and functional mapping to the various physical elements of the system. Thus, cybersecurity architectural analysis allows appropriate security mitigations to be applied where needed with rigorous justification.

After considering seminal definitions in the area, and working through the various architectural analysis approaches discussed in Section III, we present a working definition of cybersecurity architectural analysis for consideration:

> The activity of discovering and evaluating the function and form of a system to facilitate cybersecurity decisions. [31]

This definition identifies two key activities, discovery and evaluation, while simultaneously catering to both new development (i.e., a focus on desired capability through functionality) and legacy systems (i.e., a focus on existing system solutions). For new developments, discovery typically implies exploring the business or mission problem space to further understand the desired capability through functional analysis. For existing systems, this process is often conducted in reverse, mapping critical subsystems back to critical functions which support important business operations or mission execution. It is also worth noting that cybersecurity architectural analysis should also help with identifying and understanding how security requirements support the desired capability, which also provides traceability that is often lacking in systems security efforts.

As part of the broader system definition and development effort, cybersecurity architectural analysis should help inform engineering tradeoffs and decision making such as those processes and activities described in ISO/IEC/IEEE 15288.

III. CURRENT CYBERSECURITY ARCHITECTURAL ANALYSIS APPROACHES

In this section, we survey architectural analysis approaches and assess their applicability for complex system cybersecurity. Within the DoD (and its major defense contractors), several approaches (i.e., methods, processes, and tools) have been developed to secure and assess the cybersecurity of complex systems and systems-of-systems. While providing a detailed case study for each approach surveyed in this work would be ideal for a robust assessment, it is just not feasible as some approaches take months if not years to complete. This survey is based on publicly available literature and presentations that focus specifically on architectural analysis for weapon systems.

The predecessor for many cybersecurity architectural analysis approaches is compliance-based Information Assurance (IA), which focuses almost exclusively on applying security controls to computer networks and IT systems. For complex systems, this approach is inadequate as demonstrated by several high profile security breaches [29]. This inadequacy has driven the development of many of the approaches described in this work.

A. Department of Defense Architectural Framework (DoDAF)

The integrated architecture currently in use by the DoD is the DoD Architecture Framework (DoDAF). Its purpose is to manage complexity to enable key decisions through organized information sharing [23]. However, in DoDAF, like many other architecture frameworks, security (or cybersecurity) is not specifically addressed [30]. James Richards, in his work Using the Department of Defense Architecture Framework to Develop Security Requirements [28], proposes a methodology for using DoDAF to derive security requirements. He outlines a process of first building an architectural model of the enterprise, focusing on a core set of views including the OV-5b operational activity model, the DIV-2 logical data model, and the OV-3 operational resource flow matrix. These critical views are used to model security-relevant processes, data, business rules, and communications. Next, he suggests comparing views for compliance and then assessing and refining the architecture. The overall purpose of Richards' approach is to use DoDAF to expose or derive security requirements [28], This approach has not been widely adopted, but his work demonstrates utility for complex cyber-physical systems.

B. Unified Architecture Framework (UAF)

In contrast to the unique solution DoDAF, industry has developed the Unified Architecture Framework (UAF) [31]. Based on industry need, the UAF includes a formal security domain amongst the more common architectural views. The UAF security domain includes views for security taxonomy, structure, connectivity, processes, constraints, and traceability. More specifically, it uses Systems Modeling Language (SysML) class diagrams to identify data types and map them to protections and security controls. As an integrated architecture, it allows security-relevant elements to be mapped to system resources and operations. UAF also capitalizes on the success of model-based sytems engineering (MBSE) efforts to depict and analyze the security properties of a simulation oriented language (SoI) via an executable architecture. Note, UAF is in the final stages of development, so its utility has yet to be fully realized; however, some pathfinder examples of proposed security views demonstrate utility for conducting cybersecurity architectural analysis of complex cyber-physical systems [32].

C. Publically Available Industry Efforts

Major defense contractors often use custom architectural analysis approaches to design and evaluate their system architectures concerning cybersecurity. Although it is likely that most large DoD contractors are working solutions in this area; at the time of this survey, the authors were only exposed to efforts from Raytheon, Northrop Grumman, and Lockheed Martin. Note, Raytheon's Cyber Resiliency Architecture Framework (CRAF) was the only approach with a detailed open-source publication available. Limited information is available on Northrop and Lockheed's approaches.

Raytheon developed CRAF using a DoDAF reference architecture with extensions for specific cyber resilience mappings and metrics [33]. The goal of CRAF is to assess and identify gaps in cyber resiliency by mapping systems, subsystems, and components against prioritized capabilities to identify resilience requirements for critical mission scenarios.

Using failure modes and effects analysis, Northrop Grumman created a risk-based assessment methodology using an integrated architecture modeled in the new UAF to identify cyber risks for their systems [32]. This approach is still under development and is one of the first systems security efforts based on the upcoming UAF standard security views from the Object Management Group (OMG).

Lockheed Martin has created a custom solution titled the Secure Engineering Assurance Model (SEAM) [34]. SEAM is a tailored systems security engineering approach to integrate security into every solution they deliver. This framework provides tailored security considerations and checklists for each program area.

D. Risk Management Framework (RMF) for Cybersecurity

In response to increasing risks against critical infrastructure and information technology systems, the US government enacted the Federal Information Security Management Act of 2002 which established minimum information security requirements for federal information systems, and charged the National Institute of Standards and Technology (NIST) with developing security standards and guidelines to address these growing risks [35]. In response to this requirement, NIST created the Risk Management Framework (RMF) which provided a structured yet flexible process for applying these standards and guidelines [36]. Accordingly, RMF is the mandated approach for addressing cybersecurity in the DoD [11]. In general, this approach applies a prescriptive risk-based methodology to cybersecurity with the goal of identifying, mitigating, and eliminating system vulnerabilities to protect systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Within the U.S. Air Force, the Air Force Life Cycle Management Center is tasked with conducting RMF for legacy weapon systems (designated as the Platform IT (PIT) systems) [37]. This PIT assessment and authorization process consists of six-steps described in the next paragraph [13].

First, the team must categorize the PIT system according to the information displayed, processed, stored, and transmitted along with the classification of the information and associated technologies. Second, security controls are selected (or assigned) based on the impact resulting from the loss of said information (i.e., criticality analysis) [12]. The third step is implementing said controls with consideration for cybersecurity requirements across the entire system development life cycle—although security controls have been historically applied to IT systems, many have been tailored for PIT systems with prescribed overlays [37]. The fourth step is key to the RMF process and assesses the effectiveness of applied

security controls through threat mapping and vulnerability analysis. On a related note, much of the security work conducted today is exclusively focused on this step. Based on the identified vulnerabilities, the fifth step is to produce a risk assessment and mitigation plan, which is then briefed to the Authorization Official for authorization. The sixth step of the RMF process is continuous monitoring of the system with respect to cybersecurity. As the system and threat environment evolve, security control effectiveness needs to be continuously assessed while keeping in mind future changes and cybersecurity impact.

The RMF is the mostly widely implement approach of those surveyed as it is mandatory for DoD information systems to receive an authorization to operate. While this approach has mitigated vulnerabilities, many cite its perceived difficulty, steep learning curve, and IT-centric focus as currently implemented as critiques in its utility for complex cyber-physical systems.

E. Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) and Cyber Hardening Efforts

The Air Force Research Laboratory (AFRL), in conjunction with the Air Force Institute of Technology's (AFIT) Center for Cyberspace Research, developed an Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) Workshop [38]. This weapon-system-specific workshop teaches a thorough analysis approach by systematically identifying and assessing all external inputs and communications paths to and from a weapon system (i.e., an exhaustive boundary analysis of the system's architecture). The primary activities include gathering information, identifying and analyzing access points, finding and analyzing susceptibilities, anticipating attacks, and applying and recommending mitigations and protections. The ACVAM approach requires extensive subject-matter expert (SME) involvement, access to design documents, and detailed operator insight to discover susceptibilities and determine appropriate mitigations to increase mission assurance by eliminating or reducing vulnerability to cyberattacks. [39]

Additionally, AFRL is developing enhanced cyber hardening tools and resiliency instructions [40]. While specific details are not publicly available, the cyber hardening approach was recently briefed to the defense community at large [39]. In general, this approach describes avionics cyber hardening and resiliency concepts and suggests ways to protect avionics and related systems from cyberattack. Moreover, this approach encourages engineers to 'think avionics cyber' using three tenets of cyber protection: focus on what's critical; restrict access to the critical; and detect, react, and adapt [41]. These approaches provide a robust analysis but require technically savvy domain experts to execute, which restricts its utility for a larger group of complex systems.

F. Attack Path Analysis via Automotive Example

Historically, attack path analysis has served the security community well [42]. In a great

example from the automotive domain, Checkoway *et al.,* provide a practical attack path analysis and comprehensive discussion which solidifies the importance of threat modeling as a cybersecurity architectural analysis technique [8]. While this specific example is automobile-centric, many similarities are shared between cyber-physical systems. More specifically, the work details a four-step method of analyses. First, threat model characterization is accomplished through identification of external attack vectors and attack surfaces. Second, vulnerability analysis addresses the accessibility, criticality, and exploitability of potential vulnerabilities. Third, a threat assessment attempts to gauge the attacker's motivation by answering the question of what utility a given attack path has for the attacker. Finally, the approach suggests mitigation actions by synthesizing similarities among vulnerabilities to provide practical recommendations for enhancing the system's cybersecurity.

G. System Theory Process Analysis for Security (STPA-Sec)

In recent work, MIT's System Theory Process Analysis (STPA) approach for safety was extended to focus on security related concerns, known as STPA-Sec [43]. The goal of this approach is to ensure mission-critical functions are maintained in the face of disruption(s). Starting from a strategic viewpoint, system developers and users can proactively shape the operational environment by controlling specified mission critical system risks. This top-down approach elevates the security problem from guarding the system (or network) against all potential attack paths to a higher-level problem of assuring the system's critical functions. The STPA-Sec steps include: identifying unacceptable losses, identifying system hazards (vulnerabilities), drawing the system functional control structure, and identifying unsafe or insecure CAs [43]. This method has been embraced by defense and commercial industries with several favorable case studies [43].

H. Functional Mission Analysis for Cyber (FMA-C)

The DoD has adopted Functional Mission Analysis for Cyber (FMA-C) as an approach to secure operational computer networks [45]. FMA-C is being taught to thousands of airmen to assure critical cyber systems and reduce vulnerabilities. While the structure and content of FMA-C are similar to STPA-Sec, its application is tailored to As-Is Information Technology infrastructures. In practice, Air Force Mission Defense Teams apply FMA-C to fielded cyber systems to identify mission-critical vulnerabilities. It has proved to be a useful tool for understanding and mitigating risks in traditional cyber (i.e., ICT) domains.

I. Other Notable Methodologies

As previously noted, other methodologies and frameworks for systems-level security analysis are sure to exist which are not covered in this work. A few notable works focused on mission assurance are available here [46], [47], [48], and on software here [49], [50].

IV. DESIRABLE CHARACTERISTICS FOR CONDUCTING CYBERSECURITY ARCHITECTURAL ANALYSIS

This section identifies desirable characteristics for cybersecurity architectural analysis and cross-examines the approaches discussed in Section III.

A. Cybersecurity Architectural Analysis Characteristics

The first characteristic is definitional and classifies approaches as either top down or bottom up. Those defined as top down start with analysis at the function level with identification and examination of critical missions and/or capabilities—sometimes operations depending on how the approach is being applied. As is typical of architecting for new systems (and sometimes upgrades), higher-level functional analysis leads to further functional decomposition and allocation to a more specific form (e.g., lower subsystems, elements, or components). These approaches lend themselves to the identification of stakeholder security needs, early trade-offs, thorough security requirements definition, and integration of more holistic security solutions [27].

Conversely, bottom-up approaches begin with the form in mind (i.e., the physical or technological solution) and often focus on perimeter security through boundary analysis [51]. While this approach successfully identifies vulnerabilities in networked components, it is often less useful for protecting systems from intelligent adversaries. For example, Bayuk and Horowitz [52] surmise that perimeter defense tactics are mostly ineffective, and conclude that a top-down, risk-based systems engineering approach to system security should be used instead.

The next key characteristic is whether the approach should be driven by threats or vulnerabilities. Prior research suggests that the foundation for improving system security starts with an analysis of potential threats, which leads to more appropriate security requirements for implementation [42]. This is intuitive; without first understanding the adversary—system-specific threats (and their rapid agility)—it is difficult, or impossible, to defend against them. Understanding and modeling the threat becomes a critical prerequisite for generating and developing secure systems [53]. Once the model has been developed and validated, vulnerability analysis is the logical follow-on. With the threats understood, the system architecture can be analyzed for vulnerable access points through techniques such as attack path analysis and/or red teaming.

While acknowledging the rapidly changing nature of threats, the exercise of red teaming and brainstorming potential attack paths is a helpful critical thinking exercise for ensuring sound cybersecurity practices. Moreover, threat modeling and vulnerability analysis typically form the foundation for cybersecurity architectural analysis. While threat modeling alone does not ensure cybersecurity, rigorous threat modeling and vulnerability analysis are helpful for ensuring the security of realized systems. However, more focus should be applied to providing security solutions and not just focused on identifying problems.

In today's highly-contested cyberspace environment, documentation-based engineering is largely ineffective against dynamic adversaries [42]. Developing a successful response to a dynamic adversary necessitates the tools and methods used to develop countermeasures be, in kind, dynamic. In response to these complexities, Model-Based Systems Engineering (MBSE) offers an integrated modeling approach capable of mapping desired capabilities to functions (and even components), as well as providing traceability and fit-for-purpose views to enable more effective decision-making [54]. In a recent effort, Apvrille and Roudier proposed SysML-Sec, an injection of security considerations into SysML to foster integration between system designers and security experts [55]. SysML-Sec and more generally MBSE approaches enable security-focused computer simulations of a potential system architecture. These executable architectures provide tremendous value by providing insights into early design trade-off analysis [56]. While MBSE requires significant initial investment in tools and training, it significantly increases the depth of possible architectural analysis, especially in executable architectures.

B. Assesment of Architectural Analysis Approaches

Table I provides a consolidated assessment (i.e., a mapping) of the proposed architectural analysis characteristics to the surveyed approaches from Section III. This mapping seeks to provide a consolidated reference for differentiating approaches to inform the user and assist in selecting an appropriate cybersecurity architectural approach which meets the stakeholders' needs. Consideration is given to each approaches' usability, scalability, and tool availability. The ideal approach will also easily facilitate modeling and simulation studies to perform early design feasibility studies and support trade-off analysis (i.e., MBSE).

In general, bottom-up approaches are relatively systematic; however, historically they have not produced secure systems and tended to scale poorly. Top-down approaches have the benefit of being more scalable, but they often require a high level of tool proficiency to effectively model (thus, the potential of MBSE to systems security is largely missed). While vulnerability analysis is inherent in every approach, a threat- based approach is less so. This aspect is crucial because effectively safeguarding unprecedented, and complex systems require more than a good architectural tool or technique – a holistic engineering approach that embraces all aspects of security (e.g., people, processes, policy, technology, feasibility, cost, etc.) is required [57], [58].

V. CONCLUSIONS AND FUTURE WORK

The practice of architectural analysis is not new; however, in the context of complex cyber-physical systems, the role of architectural analysis with respect to cybersecurity is not well understood. Moreover, given cybersecurity's widespread interest, it was surprising to find a general lack of understanding or consistency regarding what it means to conduct architectural analysis for cybersecurity while surveying the literature. Thus, this work

	Top Down	Bottom Up	Threat Driven	Vul. Based	MBSE Integrated	MBSE Executable	Tool Based
DoDAF+ Richards	X[1]			X	X	X[4]	X
CRAF	X[1]		X	X	X	X	X
UAF Security	X			X	X	X[4]	X
ACVAM		X	X	X			
STPA-Sec	X[2]			X			
RMF		X[5]	X	X	X[3]		

1. Promotes a top-down approach after mission functions are identified (i.e., does not include mission thread analysis).
2. Approach begins at a higher level than other approaches examined (i.e., includes mission thread analysis) and includes lower level analysis.
3. Suggests using MBSE, but not required and often not considered.
4. Would require pairing with additional modeling and simulation plugin.
5. RMF is intended to be a top-down approach but is often applied bottom-up using security control compliance based on system type.

Table 1: Architectural Approaches to Characteristics Mapping

briefly surveys key architectural analysis concepts and provides a timely and widely applicable working definition of "cybersecurity architectural analysis" for the community to consider. Next, a survey of several cybersecurity architectural analysis approaches from industry and government is provided, along with an assessment of their applicability for complex cyber-physical systems according to several desirable characteristics. These results help practitioners and researchers understand how to achieve more effective cybersecurity architectural analysis efforts to develop secure systems according to stakeholders needs.

While there are several promising cybersecurity architectural approaches, each with unique aspects to be more fully explored, standardized approaches such as UAF paired with MBSE hold promise and have a wider acceptance than some alternatives. In the near term, the authors have chosen to explore STPA-Sec to more fully understand its utility as

a relatively simple architectural analysis approach to assist in the development of safe, secure, and resilient military systems. Specifically, the authors are executing a detailed case study for a next-generation aircraft refueling system. This case study focuses on understanding the utility of the STPA-Sec approach for eliciting cybersecurity and resiliency requirements when developing complex military systems (i.e., unprecedented cyber-physical systems of systems). Ultimately, continued research in this field will enable more effective and efficient cybersecurity architectural analysis for complex systems regardless of the application domain.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

ACKNOWLEDGMENTS

This work was supported by the U.S. Air Force, Air Force Institute of Technology, Cyberspace Center for Research, Wright-Patterson Air Force Base, Ohio, United States of America.

NOTES

1. White House, "Remarks by the President on Securing our Nation's Cyber Infrastructure," White House Press, 2009.

2. P. Singer and A. Friedman, Cybersecurity and Cyberwar, New York: Oxford, 2014.

3. Y. Liu, Y. Peng, B. Wang, S. Yao and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica,* vol. 4, no. 1, 27-40, 2017.

4. R. Saracco, "Guess What Requires 150 Million lines of Code," EIT Digital, January 13, 2016, [Online], Available: https://www.eitdigital.eu/news-events/blog/article/guess-what-requires-150-million-lines-of-code/, accessed February 2017.

5. R. Charette, "IEEE Spectrum: This Car Runs on Code," February 1, 2009. [Online]. Available: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, accessed June 1, 2017.

6. A. Greenberg, "Wired," Wired Magazine, July 21, 2015, [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed April 25, 2017.

7. E. Perez, "CNN," CNN, May 18, 2015, [Online]. Available: http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/, accessed April 25, 2017.

8. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security Symposium, 2011.

9. United States Congress, "Nation Defense Authorization Act 2016 Section 1647," November 25, 2015, [Online]. Available: https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf, accessed June 1, 2017.

10. Department Of Defense, "DoDI 8500.01 Cybersecurity," 2014.

11. Department of Defense, "DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)," 2014.

12. Department of Defense, "Defense Acquisition Guidebook Chapter 9 Program Protection," April 5, 2017, [Online]. Available: https://www.dau.mil/tools/dag/Pages/DAG-Page-Viewer.aspx?source=https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx, accessed June 1, 2017.

13. Department Of Defense, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle," October 30, 2015, [Online]. Available: https://acc.dau.mil/adl/en-US/721696/file/81323/Cybersecurity%20Guidebook%20v1.10%20signed.pdf, accessed June 1, 2017.

14. J. A. Zachman, "A Framework for Information Systems Architecture," IBM Systems Journal 26, vol. 26, no. 3, 276-292, 1987.

15. J. F. Sowa and J. A. Zachman, "Extending and Formalizing the Framework for Information Systems Architecture," *IBM Systems Journal,* vol. 31, no. 3, 590-616, 1992.

16. J. Zachman, "The Zachman Framework Evolution," April 1, 2011, [Online]. Available: https://www.zachman.com/ea-articles-reference/54-the-zachman-framework-evolution, accessed May 11, 2017.

17. A. Tang, J. Han and P. Chen, "A Comparative Analysis of Architecture Frameworks," *IEEE Computer Society: Proceedings of the 11th Asia-Pacific Software Engineering Conference,* vol. 4, no. 1530-1362, 1-8, 2004.

18. C. Paulsen, "Cybersecuring Small Businesses," *IEEE Computer,* vol. 49, no. 8, 92-97, 2016.

19. Department Of Defense, "DoDI 8500.01 Cybersecurity," 2014.

20. G. Hurlburt, "Good Enough Security: The Best We'll Ever Have," *IEEE Computer,* 98-101, 2016.

21. M. W. Maier and E. Rechtin, The Art of Systems Architecting, CRC Press, 2009.

22. ISO/IEC/IEEE 42010, "Systems and Software Engineering: Architecture Description," 2011.

23. Department of Defense, "Department of Defense Architecture Framework," 2010.

24. J. Zachman, "Wikipedia," May 5, 2010, [Online], accessed May 10, 2017.

25. R. N. Taylor, N. Medvidovic and E. Dashofy, Software architecture: foundations, theory, and practice., Wiley Publishing, 2009.

26. E. Crawley, B. Cameron and D. Selva, System Architecture, Hoboken: Pearson, 2016.

NOTES

27. R. Ross, M. McEvilley and J. Oren, "NIST Special Publication 800-160: Systems Security Engineering," National Institute of Standards and Technology, Washington DC, 2016.

28. J. E. Richards, "Using the Department of Defense Architecture Framework to Develop Security Requirements," 2014. [Online]. Available: sans.org, accessed February 2017.

29. P. Singer and A. Friedman, Cybersecurity and Cyberwar, New York: Oxford, 2014.

30. L. Ertaul and J. Hao, "Enterprise Security Planning with Department of Defense Architecture Framework (DODAF)".

31. Object Management Group, "Unified Architecture Framework Profile," OMG, 2016.

32. T. Hambrick and M. Tolbert, "Unified Architecture Framework Profile-Systems Engineering Method for Security Architectures-NMWS 17," May 21, 2017, [Online]. Available: https://nmws2017.com/agenda, accessed May 21, 2017.

33. S. Hassell, "Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of System, and Networks Against Cyber Threats," *INCOSE INSIGHT,* vol. 18, no. 1, 26-28, 2015.

34. P. Nejib and D. Beyer, "Secure Engineering Assurance Model," June 11, 2014, [Online]. Available: http://www.incose.org/docs/default-source/enchantment/140611beyernajib-lockeedseam.pdf?sfvrsn=2, accessed June 8, 2017.

35. "E-Government Act of 2002. Pub. L. No. 107-347, 116 Stat. 2899," December 17, 2002, [Online]. Available: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, accessed January 30, 2018].

36. R. Ross, "Managing Enterprise Security Risk with NIST Standards," *Computer,* 88-91, August 20, 2007.

37. AFLCMC/EZAS, "Aircraft Cybersecurity Risk Management Framework," May 19, 2014, [Online]. Available: http://www.mys5.org/Proceedings/2014/Day_2_S5_2014/2014-S5-Day2-12_VanNorman.pdf, accessed May 2017.

38. Air Force Institute of Technology Center for Cyberspace Research, "Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) Workshop," Air Force Research Laboratory, December 1, 2015. [Online]. Available: https://www.afit.edu/ccr/page.cfm?page=1184&tabname=Tab2, accessed May 1, 2017.

39. Air Force Research Laboratory, "Air Force Research Lab Avionics Vulnerability Assessment and Mitigation Efforts," in *Ohio Cyber Dialogue with Industry,* Dayton, 2017.

40. K. Osborn, "BattleSpace IT - Air Force: An F-16 could be vulnerable to cyber attack," Defense Systems, October 18, 2016, [Online]. Available: https://defensesystems.com/articles/2016/10/18/cyber.aspx, accessed May 2017.

41. J. Hughes and G. Cybenko, "Three tenets for secure cyber-physical system design and assessment," in *SPIE Defense+ Security,* 2014.

42. J. Cleland-Huang, T. Denning, T. Kohno, F. Shull and S. Weber, "Keeping Ahead of Our Adversaries," *IEEE Software,* vol. 33, no. 3, 24-28, 2016.

43. W. Young and N. G. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM,* vol. 57, no. 2, 31-35, 2014.

44. Massachusetts Institute of Technology, "MIT Partnership for a Systems Approach to Safety," March 27, 2017, [Online]. Available: http://psas.scripts.mit.edu/home/stamp-workshop-2017/, accessed June 8, 2017.

45. Air Force Cyber College, "Top-down Purpose-based Cybersecurity," 2015, [Online]. Available: https://www.sans.org/summit-archives/file/summit-archive-1492176717.pdf, accessed January 1, 2018.

46. G. Hastings, L. Montella and J. Watters, "MITRE Crown Jewels Analysis," The MITRE Corporation, 2009.

47. H. G. Goldman, "Building secure, resilient architectures for cyber mission assurance," The MITRE Corporation, 2010.

48. C. Alberts and A. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," 2005.

49. C. Alberts, C. Woody and A. Dorofee, "Introduction to the Security Engineering Risk Analysis (SERA) Framework," 2014.

50. Software Engineering Institute, "Security Engineering Risk Analysis (SERA)," CERT- Carnegie Mellon University, November 1, 2015, [Online]. Available: https://www.cert.org/cybersecurity-engineering/research/security-engineering-risk-analysis.cfm?, accessed May 1, 2017.

NOTES

51. R. Anderson, Security Engineering, 2nd ed., Indianapolis, Indiana: Wiley Publishing, Inc, 2008.

52. J. Bayuk and B. Horowitz, "An Architectural Systems Engineering Methodology for Addressing Cyber Security," *Systems Engineering,* vol. 14, no. 3, 294-304, 2011.

53. A. Shostack, Threat modeling: Designing for security, John Wiley & Sons, 2014.

54. A. Ramos, J. Ferreira and J. Barceló, "Model-based systems engineering: An emerging approach for modern systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C* (Applications and Reviews), vol. 42 , no. 1, 101-111, 2012.

55. L. Apvrille and Y. Roudier, "Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems," *Electronic Proceedings in Theoretical Computer Science,* vol. 148, no. 2, 15-30, 2014.

56. J. A. Estefan, "Survey of Model-Based Systems Engineering (MBSE) Methodologies," International Counsel On Systems Engineering (INCOSE), 2008.

57. J. Eloff and M. Eloff, "Information Security Architecture," *Computer Fraud and Security,* vol. 11, 10-16, 2005.

58. T. Patterson, "Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk," *Computer Fraud and Security,* 13-15, 2003.

The Cyber Defense Review

Book Review

Strategic A2/AD in Cyberspace by Alison Lawlor Russell

Reviewed by
Dr. Jan Kallberg and
Cadet Daniel Muncaster

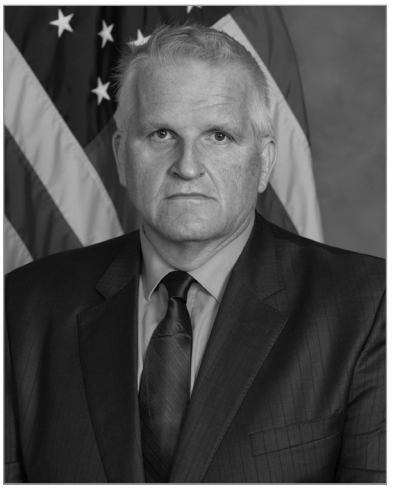
Through a concise and straightforward narrative, Dr. Alison Lawlor Russell outlines the major issues threatening the United States cyber system through the lens of an A2/AD perspective. Alison Russell is an Assistant Professor of Political Science and International Studies at Merrimack College.

How can the people of the United States defend their land and physical assets? This traditional question applies not just to American citizens, but to people across the world and throughout history. A recurring answer is the principle of Anti-Access/Area Denial or A2/AD.

The A2/AD strategy is defined as refusing "movement to a theater (anti-access), while [area denial] affects movement *within* a theater." Putting these ideas into context, A2 would be the US blocking the Soviet Union's access to Cuba with a naval quarantine; AD would be hampering the enemy's ability to maneuver in the Mekong Delta, such as guerilla tactics against US forces in Vietnam.

These strategies represent some of the traditional levels of conflict in cutting communication lines or sequestering the opponent. The world, however, is changing, and conflict changes with it. Cyberspace now plays a crucial role not just in economic and social situations, but also in military communications.

Dr. Russell, in *Strategic A2/AD in Cyberspace,* discusses these concepts and defines cyberspace as one of the current *centers of gravity* around which global strategy now



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.

orbits. The Internet, Dr. Russell states, is a significant vulnerability to American society as the primary communications network used for daily life. Within this vulnerability, however, lies the opportunity to leverage power against opponents. Here, Dr. Russell focuses her research entirely on the growing importance of cyberspace and its implications for the global balance of power.

The book is less convincing when it goes through different layers of the Open Systems Interconnection model (OSI model) and puts each layer into the A2/AD context, which might work as a systematic way to approach the topic, but does not carry the discourse the whole way forward. The Internet is designed to trace new routes in a degraded environment, as its core design was tailored to ensure the survivability of information resources in a nuclear war, so the question is whether an adversary could be in total command of the physical layer—the Internet conduit—to execute A2/AD operations. Dr. Russell's *Strategic A2/AD in Cyberspace* has merits in the discourse on whether previous A2/AD discussions have a bearing on cyber and provides a good understanding of how and why A2/AD might be relevant to cyber. The book projects a strategic outlook—the national security perspective—but repeatedly dips into tactical territory, discussing cyber hygiene and minor events. Of the concerns raised in the book, three stand out as highly relevant today: satellites, undersea cables, and electromagnetic pulses. All three are known concerns, but Dr. Russell puts them in another context that is worthy of reflection.

Dr. Russell proposes policy and strategic guidelines to help ensure the United States is well prepared for any attack on its most crucial communications network, and can deter cyber aggression in the future. The book's weakness is that the policy advice

Cadet Daniel Muncaster is a rising Yearling at West Point, and is majoring in International History with a minor in Grand Strategy. This past summer he went to Air Assault School, Cadet Field Training, and the FBI Crisis Negotiation Course held at West Point. He is originally from Joliet, Illinois, and is a member of his Company Sandhurst team. He takes a special interest in cyber warfare and its effect on policy and national security, which he explores with his professor and mentor, Dr. Kallberg. Upon graduation, he hopes to branch Infantry or Military Intelligence.

is generic, and does not add any new viewpoints to the discourse; an example is that there should be investments in the robustness and resilience of the critical infrastructure.

Alison Russell's *Strategic A2/AD in Cyberspace* is worth reading as a short commentary on A2/AD reasoning and serves that purpose well, but its contribution to the cyber discourse is limited.

Strategic A2/AD in Cyberspace

Author: Alison Lawlor Russell

Publisher: Cambridge University Press (February 1, 2017)

Hardcover: 108 pages

Language: English

ISBN-10: 1316629627
ISBN-13: 978-1316629628

Price: $29.00

THE CYBER DEFENSE REVIEW

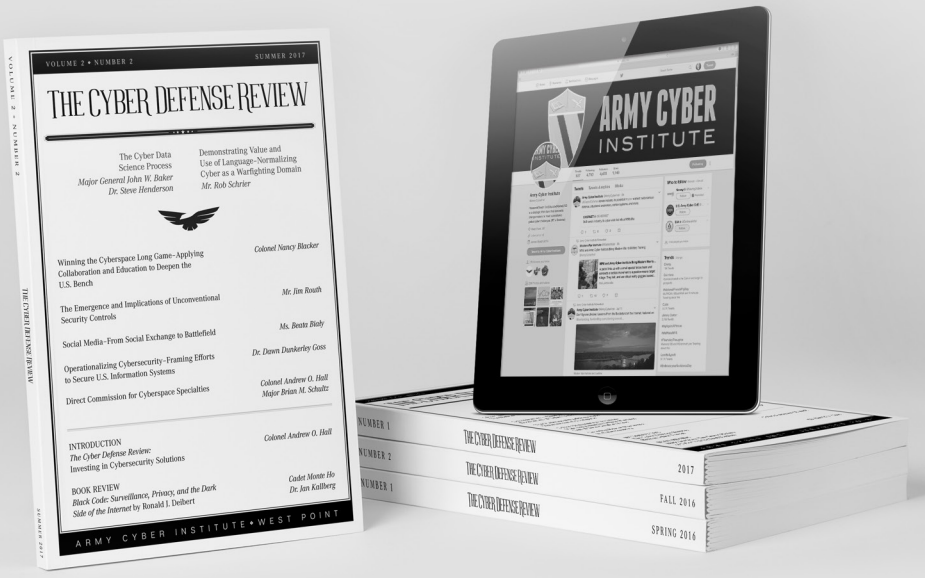
CONTINUE THE CONVERSATION ONLINE

cyberdefensereview.army.mil

AND THROUGH SOCIAL MEDIA

Facebook @armycyberinstitute

Twitter @ArmyCyberInst



ARMY CYBER INSTITUTE • WEST POINT

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