Open Access License Notice

This article is © its author(s) and is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). This license applies regardless of any copyright or pricing statements appearing later in this PDF. Those statements reflect formatting from the print edition and do not represent the current open access licensing policy.

License details: https://creativecommons.org/licenses/by/4.0/

Cybersecurity Education: A Mandate to Update

W. V. Maconachy, Ph.D
Chairman of the Board
The Colloquium of Information Systems Security Education

D. Kinsey, Ph.D
Vice Chairman of the Board
The Colloquium of Information Systems Security Education

Abstract—Recent cyber events within the U. S. cyber ecosystem present the alarming fact that attacks with both denial of service and kinetic consequences are now prevalent in non-governmental systems. This paper examines the need to expand studies of cyber and other warfare modalities into the cybersecurity curricula now being taught in American universities.

Keywords—cybersecurity, defense, education, cyber warfare

I. INTRODUCTION

Along the recognized axiom of cybersecurity defense is the realization that, in the final analysis, "any defense in depth program must account for technology, operations, and people [1]." Since that IEEE paper was published, much attention has been given to all three of those countermeasures. In particular, the people component has benefitted by a long overdue plethora of programs and resources. The nation now has Cybersecurity Centers of Excellence [2], Education Standards for teaching cyber security [3], and scholarships for the study of cybersecurity [4]. Is this enough? Are we, as a nation, indeed as an international cyber community fully prepared for the increased onslaught of cyberwarfare?

The time and era wherein corporations simply bought insurance to cover losses due to cyber attacks is now past. "The most recent important takeaway from the recent spate of ransomware attacks on US, Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively [5]." When a company or industry's core business operations are disrupted, the resultant effects, such as loss of confidence by consumers, will have a cataclysmic effect on continuity of services. This dissuades consumers from using the products of the affected company and/or causes massive disruptions to the everyday lives of citizens.

In a July 2021 report from The Center for Security and Emerging Technology the depth and spread of Chinese build up in cyber defense and offence was described as follows:

> *International competition forged China's commitment to growing its cyber capabilities. Despite a deficit of 1.4 million cybersecurity professionals, China is already a near-peer cyber power to the United States. Still, the current shortfall leaves China's businesses and infrastructure vulnerable to attack, while spreading thin its offensive talent. The NCC will likely bolster China's capabilities, making competition in the cyber domain fiercer still. U.S. policymakers should expect that China's increased capabilities will threaten the U.S. advantage in cyberspace [6].*

The report goes on to provide an outlook into the number of cybersecurity professionals to forecast for development thru the Center:

> *The NCC's "leading mission" is the National Cybersecurity School, whose first class of 1,300 students will graduate in 2022. CCP policymakers hope to see 2,500 graduates each year. The length of time it will take to reach full capacity remains unclear. The Talent Cultivation and Testing Center, the second talent-focused component, offers courses and certifications for early-and mid-career cybersecurity professionals. The Talent Cultivation and Testing Center has the capacity to teach six thousand trainees each month, more than seventy thousand in a year at full capacity. Combined, both components of the NCC could train more than five hundred thousand professionals in a single decade. [7]*

Given the past approach of China, just one of several nation states to conduct cyber warfare, the intent of the program is clear; produce significant numbers of defensive and offensive cyber personnel capable of overwhelming any target on the globe. What will the U. S. and other nations do to counter and prepare for this potential massive threat? A May 2021 Executive Order from the White House [8] follows a long string of federal attempts to secure federal networks:

> *"But cybersecurity requires more than government action. Protecting our nation from malicious cyber actors requires the federal government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built to operate securely, and partner with the federal government to foster a more secure cyberspace [8]."*

While this order presents a host of actions to be taken by the government to secure its cyber space and operations, the fact remains that "About 90 percent of the nation's critical infrastructure is owned by the private sector, and therefore is not under the control of the U.S. government or military [9]."

Who can mandate, or by what forces can the owners of the greater cyber infrastructure demand protection? The awareness of the fragility and vulnerability of the greater private cyber infrastructure has now been brought out into the full light of day by recurrent ransomware attacks. Previously, corporations, that were victims of this form of attack in an effort to keep trust in their systems and products, simply paid the ransom, often using insurance. Due to the increase of attacks, the economic forces have now come to place pressure on government and private sector alike to secure cyber networks on a global scale.

Where does the impetus for such active improvement begin? We contend, that this begins in the cyber education being delivered to students around the globe. Students, upon matriculation from cybersecurity programs enter the workforce, they must bring with them the inculcated cultural awareness that responsibility for safe cyber environments is and must be a deeply embedded government and private sector ethic.

As stated in this year's Annual Threat Assessment from the Office of the Director of National Intelligence, "During the last decade, state sponsored hackers have compromised software and IT service supply chains, helping them conduct operations — espionage, sabotage, and potentially prepositioning for war fighting [10]." This means that students must enter the workforce fully aware that many cyber-based systems have already been penetrated. The very technology that is employed in an organization can already be compromised through faulty or intentional manipulation in manufacturing, hijacked or modified orders, "the proliferation of smart products with embedded code and sensors [11]." Thus, the attribute of *trust but verify* is an essential component for all cyber security personnel. Two examples of such prepositioning include some 18,000 organizations, including nine U.S. government agencies, breached last year in the Solar Winds hack, for which Russia is widely believed responsible. The second example is the hack of the Microsoft Exchange email system that penetrated thousands of U.S. organizations, though it has received much less attention than the Solar Winds breach and many cyber experts say China is believed to be responsible.

Nation-state hackers are not limited to China. The Kaseya Ltd. breach from this past July, is believed to have been perpetrated by REvil, a Russian-linked gang [12]. The breach is considered 'one of the largest reaching ransomware attacks on record'12 and came with a demand for '$70 million in Bitcoin for a universal decryptor [12].' This is not an isolated attack by a Russian entity. Previous exposure by several cybersecurity experts including Brian Krebs identified unique signatures in ransomware that distinguishes and bypasses systems identified through language and components to be Russian.

Where does all of this lead those responsible for designing, delivering and evaluating cybersecurity education and training? It is time for updating national and global cybersecurity education and training programs. The first step in this change begins with preparing future cybersecurity practitioners and leaders with the belief that we have truly entered an era of global cyber warfare. For some academic institutions this will be an enormous change of ethos for preparing students for warfare. The need for this departure nonetheless is now upon us.

While the term cyber warfare has been with us for many years, it is most often described in terms of government operations and advanced persistent threats. Often descriptions of cyber warfare point to government-to-government conflict, "Cyber warfare refers to cyber attacks executed by one country or state against another [13]." However, companies such as the RAND Corporation describe cyber warfare as, "involving the actions by a nation-state or international as the RAND Corporation describe cyber warfare as, "involving the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks [14]." This is a broader approach to include both government and private sector networks. As with any form of warfare, the effects and damage often reach deep into the civilian populations.

In his text, Cyberwar: The Next Threat to Cybersecurity, Richard Clark notes:

> *While it may appear to give America some sort of advantage, in fact cyber war places this country at greater jeopardy than it does any other nation. Nor is this new kind of war a game or a figment of our imaginations. Far from being an alternative to conventional war, cyber war may actually increase the likelihood of the more traditional combat with explosives, bullets, and missiles. If we could put this genie back in the bottle, we should, but we can't. Therefore, we need to embark on a complex series of tasks:* ***to understand what cyber war is, to learn how and why it works, to analyze its risks, to prepare for it, and to think about how to control it [15].***

Now, ten years, and multiple government reports later, the owner of 90 percent of the cyber infrastructure may finally be poised to take action; action taken, not because of warnings, but because of open public disclosure and negative effect on a large percent of the populations. The Colonial Pipeline attack [16] may very well be the catalyst for change. The question now remains, how well is the private sector prepared to take on this challenge? One answer is that the era of cyberwarefare, while upon us, is just the prelude to what some are describing as hyperwar. What makes this new form of warfare unique is the unparalleled speed enabled by automating decision making and the concurrency of action that become possible by leveraging artificial intelligence and machine cognition.

In military terms, hyperwar may be redefined as a type of conflict where human decision-making is almost entirely absent from the observe-orient-decide-act (OODA) loop. As a consequence, the time associated with an OODA cycle will be reduced to near-instantaneous responses.

As the "OODA loop is what happens between the onset of a stimulus and the onset of a reaction to that stimulus[17]." With the reaction time differing between known and unknown stimulus, building a base of understanding through detailed, hands-on application in the classroom and addressing the need to create automated programs and tools to more quickly assess stimulus is essential. The implications of these developments are many and game changing.

The employment of offensive cyber systems will rapidly render useless sensors and air defenses fielded by less sophisticated foes. The traditional SEAD [Suppression of Enemy Air Defenses] mission and use of stealth **jets may in some cases be obviated by a cyber payload** putting a SAM [surface-to-air missile] site out of commission without a shot being fired or a single life being risked [18]. Understanding this complex attack and defend methodology has been in the purview of defense departments around the world.

Given the crippling effect of cyber attacks as a part of a larger scale offensive upon a nation's critical infrastructures, is it time to take such learning into the broader cybersecurity practitioner's education? In short, practitioners of cyber defense must learn how to operate in a hyperwar environment. If so, what might some of the elements of that study include? It is no longer unimaginable that cyber systems will be breached at the same time communications networks, power networks, and other elements of the nation's critical infrastructure simultaneously fail. Add to that a catastrophic kinetic attack, and students as well as current practitioners must experience reconstitution of systems within that complex environment.

Before a study of that content can be undertaken, the government must, as stated in the President's Executive Order on improving our nation's cyber security [19], develop a program for sharing cyber threat information. Once the nature, direction, and sources of those threats are shared, students can begin to organize their studies around threat and risk analysis. A proven instructional method for achieving that mastery is via structured attack and defined scenarios as now practiced in several collegiate cyber competitions [20]. Often described as cyber capture the flag [CTF] competitions, students will develop the skills needed for defending a given cyber environment and develop a keen sense for building cyber defenses in the context of cyber ecosystems.

CTF activities are easily scaled for any cyber security educational level due to the vast offering of challenges varying in degree of difficulty, tools and techniques used, and goal to achieve (such as finding a 'flag') [21]. Changing the time available for a challenge can also significantly impact the level of difficulty in achieving a successful outcome. This is not a new concept.

> *"Like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non - profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes. Today in cyberspace, intelligent adversaries exploit vulnerabilities and create incidents that propagate at machine speeds to steal identities, resources, and advantage. The rising volume and virulence of these attacks have the potential to degrade our economic capacity and threaten basic services that underpin our modern way of life [22]."*

In March 2020, the Cyberspace Solarium Commission noted that, "A major cyber attack on the Nation's critical infrastructures and economic system would create chaos and lasting damage exceeding that wreaked by fires in California, floods in the Midwest, and hurricanes in the Southeast [23]." This report, coming from Congress, offers hope and direction for preparing our nation for a catastrophic attack. The report presents recommendations for six pillars for shoring up our cyber defenses:

- Pillar 1: Reform the U. S. Government's structure and organization for cyberspace.
- Pillar 2: Strengthen norms and non-military tools
- Pillar 3: Promote National resilience
- Pillar 4: Reshape the cyber ecosystem toward greater security
- Pillar 5: Operationalize cybersecurity collaboration with the private sector
- Pillar 6: Preserve and employ the military instrument of power [24]

Where this study, with findings and recommendations differs from past studies is that this proposal comes from congress and not the executive branch. Congress provides funds.

All of this needed change is only achievable if a climate and culture of trust and collaboration is enabled. This is difficult to do between often competing organizations much less between certain factions of business and industry with government. The reverse is also true with government operating in an environment of trust with private sector. Here, education can play a significant role. In addition to teaching requisite cyber knowledge and skills, education is the perfect medium for enabling the attribute segment of the Knowledge, Skill, and Ability continuum. Here, the active collaboration and support of both government and business with academia is critical. Schools need up-to-date equipment, current threat analysis, and insights into government / industry collaborations for improving cyberspace. On this note, none of the calls for action to date include folding academia into government and private sector collaborations.

II. Summary of Suggestions

Changing the way we teach cybersecurity concepts can be difficult as faculty have many students, little time, and a multitude of responsibilities. To make inclusion easier we offer the following suggestions:

- Teach cyber security in the context of operating in a cyberwar environment. An inclusion that could generate discussion and research into this topic would be asking students to compare and contrast three differing nation's approaches to cyberwarefare. A natural segue from this is to ethical considerations of cyberwar and protection of assets.
- Increase use of capture the flag practical exercises, but include elements of hyperwar. This prepares students for the unexpected, challenges them in individual and team-based competitions for a common goal, and offers the opportunity to experience a 'crisis mode' of operation not normally present in classroom activities. Most participants realize the gaps in their understanding based on their success and accomplishments in CTF activities much more quickly than if left to a school then work progression.
- Teach cyber security with a modified OODA loop approach, emphasizing constant vigilance. This can be included in cyber security preparedness. Students should be able to list the actions necessary to identify and respond to a cyber breach, such as if it were their research material.
- Include academia in any government – private sector collaborations, to include, where possible, sharing of threat analysis information. Faculty could invite government speakers to address equities issues. Class-based interviews of industry cybersecurity leaders could be made to assess what impediments to full trust exist between industry and government information sharing.
- Increase teaching and understanding of the threats in supply chain management. Synergistic partnerships between cyber and logistics programs could benefit both when faculty share expertise with their counterparts and both programs are enhanced.
- Develop programs with greater emphasis in instilling the attributes needed for individuals to operate in the highly vulnerable cyber environment. Focusing on actions and competencies instead of terminology and knowledge.
- Develop and teach cyber operations in the context of cyber ecosystems. Researching national authorities for conducting cyber counter attacks is one approach.

REFERENCES

[1] W.V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A Model for Information Assurance; An Integrated Approach," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, N Y. 5-6 June. P1.

[2] NSA. Centers of Academic Excellence. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

[3] National Institute of Standards and Technology. Mapping NSA/DHS Knowledge Unit to NICE Framework 2.0. https://www.nist.gov/system/files/documents/2017/06/14/nsa_dhs_cae_ku_mapping_to_nice_fw_2.0.pdf.

[4] OPM. Washington, D.C. https://www.sfs.opm.gov/.

[5] The White House. Memo to Corporate Executives and Business Leaders. "What We Urge you to do Against the Threat of Ransomware. June 2, 2021.

[6] Center for Security and Emerging Technologies. China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain. Dakota Cary. July, 2021. https://doi.org/10.51593/2020CA016.

[7] Ibid

[8] The White House. Executive Order on Improving the Nation's Cybersecurity. May, 2021.https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[9] U. S. News. NSA Chief Says U. S. Infrastructure Highly Vulnerable to Cyber Attack. https://www.reuters.com/article/us-usa-cybersecurity/nsa-chief-says-u-s-infrastructure-highly-vulnerable-to-cyber-attack-idUSBRE95B10220130612. June 12, 2013.

[10] Office, Director of National Intelligence. Annual Threat Assessment of The U S Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. Washington, D. C. March, 2021.

[11] Gartner. Combat Digital Security Threats to the Supply Chain. Aug 19, 2020. https://www.gartner.com/doc/reprints?id=1-2570TZUW&ct=210210&st=sb

[12] Bloomberg. Kaseya failed to address security before hack, ex-employees say July 10, 2021 https://www.bloomberg.com/news/articles/2021-07-10/kaseya-failed-to-address-security-before-hack-ex-employees-say

[13] Infosecurity Magazine. https://www.infosecurity-magazine.com/blogs/cyberwarfare-frontier-wars/. May, 2021.

[14] RAND Corporation Cyberwarfare. https://www.rand.org/topics/cyber-warfare.html. SNT Monica, CA.

[15] R. Clark. Cyberwar: The Next Threat to Cybersecurity, and What to do About It. Ecco Publications. August, 2011.

[16] D. E. Sangar and N. Perlroth, New York Times. Pipeline Attack Yields Urgent Lessons About U. S. Cybersecurity. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. May 14, 2021.

[17] Boyd's OODA Loop and how we use it. 2021. https://www.tacticalresponse.com/blogs/library/18649427-boyd-s-o-o-d-a-loop-and-how-we-use-it

[18] M. T. Klare, Lobelog, The coming of Hyperwar, https://lobelog.com/the-coming-of-hyperwar/.

[19] Ibid with government.

[20] 2U, Inc. The Big List of Cybersecurity Competitions and Challenges, https://computersciencems.com/resources/cyber-security/cyber-security-competitions-list/.

[21] E. Brown. AT&T Business CTF Hacking: What is Capture the Flag for a Newbie? Dec 23, 2019. https://cybersecurity.att.com/blogs/security-essentials/capture-the-flag-ctf-what-is-it-for-a-newbie

[22] Department of Homeland Security. Enabling Distributed Security in Cyberspace. https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf. Washington, D. C. March 2011.

[23] U.S. Cyberspace Solarium Commission. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view. March, 2020.

[24] Ibid