Military Cyber Affairs

Volume 5
Issue 1 *HammerCon 2022 Special Issue*

Article 4

May 2022

The IWAR Range + 21 Years: Cyber Defense Education in 2022

Joseph H. Schafer
National Defense University

Chris Morrell
United States Military Academy

Ray Blaine
United States Military Academy

The IWAR* Range + 21 Years: Cyber Defense Education in 2022

Joseph H. Schafer, Christopher Morrell, and Raymond Blaine

Abstract

Twenty-one years ago, The IWAR Range paper published by the Consortium for Computing Sciences in Colleges (CCSC) described nascent information assurance (now cybersecurity†) education programs and the inspiration and details for constructing cyber ranges and facilitating cyber exercises. This paper updates the previously published work by highlighting the dramatic evolution of the cyber curricula, exercise networks and ranges, influences, and environments over the past twenty years.

Introduction

Twenty-one years ago, the IWAR Range paper published by the Journal of the Consortium for Computing Sciences in Colleges (CCSC‡) described nascent cybersecurity education programs and the inspiration and details for constructing cyber ranges and facilitating cyber exercises.[30] This paper updates the previously published work by highlighting the dramatic evolution of the cyber curricula, exercise networks and ranges, influences, and environments.

In 1997, the EECS department's Artificial Intelligence Research Office transformed into the cyber center—originally called the Information Technology and Operations Center (ITOC). During the summer of 1999, the Information Warfare Analysis and Research (IWAR) Range was architected and constructed in partnership with the National Security Agency (NSA) and the Defense Advanced Research Project Agency (DARPA) to enable a capstone learning experience for the newly created Information Assurance course.[12]

The ITOC's IWAR Range drove challenge-based and active learning in cyber education through real-world exercise challenges and inspired undergraduate and graduate programs around the country and around the world.[19] The ITOC forked, as illustrated in Figure 1, into the Cyber Research Center (CRC)—which provides cadets and faculty with cyber research opportunities—and the Army Cyber Institute (ACI)—which develops intellectual capital through impactful partnerships and interdisciplinary research, such as the Jack Voltaic Cyber Research Project[2] described in the Military Cyber Professional Association's (MCPA) Lockdown Lunch & Learn (3L) by

* Information Warfare Analysis and Research (IWAR) [30]

† In 2014, DoD adopted "cybersecurity" instead of "information assurance." [34:1]

‡ Formerly the Consortium for Computing in Small Colleges [6]

the ACI Director.[17] ACI also publishes the respected journal, Cyber Defense Review [4], and hosted the first Joint Service Academy Cyber Security Summit (JSAC).[15]

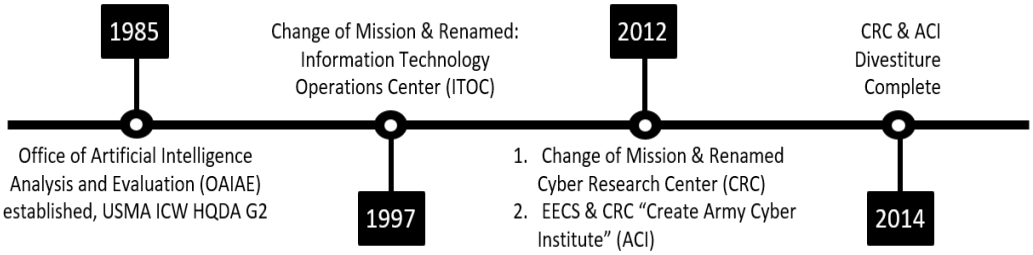

Figure 1: West Point Cyber Research Center Timeline. [8]

The authors will describe pioneering cyber activities with direct and indirect influences, the cyber curricula evolution, the IWAR Range transformation, and thoughts on the future of defense cyber education in the following sections.

Pioneers in Defense Cyber Education

Twenty years ago, cybersecurity as an academic discipline was novel. While the ITOC at West Point was pioneering cyber ranges and exercises, the U.S. Department of Defense (DoD) graduate schools such as the Naval Postgraduate School (NPS) and the Information Resource Management College (IRMC) [now the College of Information and Cyberspace (CIC)] at the National Defense University (NDU)] explored cybersecurity at the graduate and workforce / strategic levels, respectively.

Cyber Recognition and Credibility

Due to the collaboration in creating the IWAR Range, DARPA invited the IWAR Range to connect to their Information Assurance and Security Virtual Private Network (VPN), the only undergraduate institution to achieve this distinction.

In 1999, the National Security Agency (NSA) designated seven respected universities as Centers of Academic Excellence (CAE) in Information Assurance Education.[22] The following year, NSA designated seven more including the first two DoD graduate schools, NPS and IRMC / CIC at NDU.[23] In 2001, West Point became the first undergraduate-only college to receive this designation.[24]

Cyber Conferences

The research and practical exercises enabled by the IWAR Range enabled the ITOC to establish one of the first academic conferences devoted to cybersecurity, the IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop (IAWS). These workshop conferences were initiated and hosted by ITOC at West Point from 1999 through 2007.[13] These conferences were succeeded, directly and indirectly, by numerous conferences including the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) International Cyber Conflict (CyCon) conferences beginning in 2009.

The College of Information and Cyberspace (CIC) at National Defense University (NDU) began hosting Cyber Beacon (CB) in 2014. In December 2020 CIC hosted the 7th annual flagship conference virtually due to the pandemic. The theme was, "Disruption in an Era of Great Power Competition." Cyber Beacon has attracted participation from senior White House officials and the Commander of U.S. Cyber Command. CB 2020 attracted luminaries such as Congressional Cybersecurity Caucus Co-Chair, Rep. Jim Langevin; Cyber Solarium Commission Executive Director, Mark Montgomery; and DEF CON and Black Hat founder, Jeff Moss.[20]

In 2016, a collaborative effort between the ACI and CCDCOE launched the "CyCon U.S." conferences as a complement to the CyCon conferences held in Estonia. Also in 2016, ACI partnered with Citigroup on a cyber exercise called Jack Voltaic (JV). JV continues to serve as a conference, exercise, experiment, and framework to "prepare, prevent, and respond to multi-sector cyber-attacks on major cities," by partnering with players across critical infrastructures such as first responders, emergency management, transportation, telecommunications, power, water, finance, and healthcare workers.[1]

Cyber Ranges and Exercises

Jeff Moss founded DEF CON, the premier hacker conference, in 1993 and the understanding of cybersecurity as a profession evolved dramatically over the next several years.[18] For instance, in 1995, SGI Corp cyber researcher, Dan Farmer, developed the first vulnerability scanner with a web user interface, provocatively named SATAN (Security Administrator Tool for Analyzing Networks). Believing hackers would use it to break into computers, he was fired.[10] Three years later in 1998 at DEF CON 6 the hacker group, "Cult of the Dead Cow," released a "remote administration" tool called "Back Orifice" that exploited security weaknesses and allowed complete remote access to MS Windows machines.[28]

In 1999, the IWAR range included SATAN, Back Orifice, and other "hacker" and cyber security tools for use in exercises and competitions such as cybersecurity "Capture the Flag" (CTF) contests. "DEF CON CTF is one of the (if not the) oldest CTF that continues to run today." CTFs began at DEF CON 4 in 1996.[36]

The IWAR Range also motivated a proliferation of DoD Cyber Ranges including the DoD Cyber Range operated by the U.S. Marine Corps near Quantico, VA.[11] Beginning in 2011, DAPRA's National Cyber Range project has overseen prototypes of "virtual firing ranges" which model the Internet and allow researchers to simulate attacks by adversaries.[5] DoD and the recently awarded $93M contract to upgrade the national cyber range to support testing of major DoD acquisitions and facilitate U.S. Cyber Command Cyber Mission Force (CMF) rehearsals.[3]

The CMF also identified the need for a shared persistent cyber range during Exercise CYBER FLAG 2015. Cyber mission operators leveraged agile acquisition to rapidly deploy the Persistent Cyber Training Environment (PCTE) which is also being modernized.[35]

Internationally, the NATO CCDCOE organizes an annual event, Locking Shields, which is an international live-fire cyber exercise. As with ACI's Jack Voltaic, these exercises are increasingly focused in non-IT systems and the information rather than traditional computers to train and educate partners.[27] Many of these conferences and exercises can trace their heritage to the original IWAR cyber range.

Indeed, many cyber ranges, centers, educational programs, and entrepreneurial companies were founded by EECS faculty (in addition to the authors) from that time. For instance, Principal Director for Cyber in the Office of the Under Secretary of Defense for Research and Engineering, Daniel Ragsdale served in the ITOC when the IWAR range was created and went on to serve as ITOC Director and also establish the Texas A&M Cybersecurity Center. Dan was succeeded at A&M by EECS faculty member, Drew Hamilton who founded Cyber Centers at Auburn and Mississippi State.[33]

Greg Conti was Founder & Director of the Army Cyber Institute (ACI) when the ITOC was succeeded by ACI and the EECS Cyber Research Center (CRC). EECS faculty, Joe Adams led the creation of the Michigan Cyber Range and served as CIO of NDU.[16] EECS ITOC faculty Ed Sobiesk continues service at ACI. The Virginia Cyber Range was inspired by our work at West Point also; David Raymond founded the Virginia Cyber Range (virginiacyberrange.org) and is Director of the U.S. Cyber Range (uscyberrange.org). [9]

Information Assurance to Cyber Sciences

IWAR was the foundational mechanism for the creation of more formal cyber education at the Academy. The first significant dividend from this growing effort and excitement for cyber was the creation of a formal club. The growing excitement for all things cyber by what was coined the "friends of the ITOC" led to the formal creation of an Association of Computing Machinery (ACM) chapter of the Special Interest Group on Security, Audit, and Control (SIGSAC) in 2002. In the mid-2000s this excitement went mainstream with the creation of a general education requirement for a junior level information technology course. This course has evolved multiple times through the years, but has always focused on sensing, collecting, transmitting, and protecting data to gain informational advantage. Finally, the EECS Department's demand for a less theory based and more hands-on major ultimately led to the creation of Information Technology (IT) and Cyber Sciences majors in addition to the more traditional Electrical Engineering and Computer Science majors.

Cyber Educational Contests

Beginning in 2001, in coordination with NSA, ITOC organized intercollegiate CTF-type contests. The winners of these NSA Cyber Exercises were fairly balanced between the service academies[§] and these exercises encouraged a host of cyber educational contests including the National Collegiate Cyber Defense Competition (CCDC) launched in 2006 [7].. The USMA Cadet Competitive Cyber Team (C3T), formed in 2013, was a regional CCDC finalist in two of the past three years.[21]

The growing cyber infrastructure demands of SIGSAC, research, cyber competitions, ABET accredited IT and Cyber Science majors spawned more IWAR like efforts. The demand for a laboratory to support hands-on education of basic networking and network services was one of these major efforts. Department faculty leveraged the resources they had to acquire equipment and filled remaining needs by leveraging discarded equipment from across the Academy. This effort was very similar to the creation of IWAR. Eventually, courses were offered that provided hand on experience configuring network appliances like switches, routers, and firewalls. This allowed for a more hands-on approach to teaching network programming and protocol implementation.

[§] U.S. Military Academy (USMA), U.S. Air Force Academy (USAFA), U.S. Merchant Marine Academy (USMMA), U.S. Naval Academy (USNA). CDX (Cyber Defense Exercise from 20012017, NSA Cyber Exercise (NCX) from 2018 to present.[26] 2020 cancelled due to COVID-19 Pandemic, virtual in 2021, and hybrid in 2022.[25]

Lifecycle management of this type of equipment and a procurement plan based on foraging were not sustainable. However, these courses demonstrated their effectiveness and popularity, cementing their place in the curriculum. This was the genesis of the new IWAR Range.

Expanding the IWAR Range

The growing excitement for cyber in both the student and faculty populations led to inclusion of these topics in more traditional computer science and information technology courses. There was also an increase of cyber related elective courses. This constant evolution of courses to keep pace with an emerging cyber discipline required significant flexibility in pedagogy as well as resourcing. The method of building a laboratory or classroom via borrowed parts would no longer be a viable solution. The EECS Department saw this growing need and invested research funds into the infrastructure necessary to provide this flexibility. This was the beginning of the EECS cyber research network discussed in the next section.

The IWAR Range to EECSNet to WREN

The creation of the IWAR range in 1999 was the catalyst that began a movement towards cyber education and competitions at West Point. That movement drove the need for IT infrastructure capable of supporting those ideas. Ultimately, this need resulted in the creation of the West Point Research and Education Network (WREN), which has the IWAR Range at its heart.

Evolution

The IWAR Range began as a lab of approximately 37 machines with limited use of computer virtualization and has since evolved into a fully virtualized environment capable of supporting more than 1,000 concurrent machines in many different configurations. To get from its meager beginnings, IWAR went through a few major transitions over the past 20 years.

The first major upgrade to IWAR happened in 2007 and was a move to a proper datacenter and a transition to rack mounted hardware rather than its original configuration which was primarily stored in classrooms. This upgraded version of the IWAR Range continued to be physically separated from the Internet but moved to significantly higher-powered equipment. As described in the original paper[30], much of the hardware used to create the IWAR Range was no longer useful and being readied for disposal. That tradition continued in this upgraded lab, as there was no formal budget that would permit the procurement of more appropriate hardware. While the IWAR range was being relocated and upgraded, a second lab was built in the EECS academic building which was designed to support the network and network services curriculum. This new

network was like the IWAR Range in that it was physically separated from the Internet and built using primarily used equipment. It was in this configuration that the IWAR Range supported USMA's 3-time Cyber Defense Exercise win streak.

In 2015, the IWAR Range and the networking curriculum labs were connected to enable compute and network resource sharing. This combined network became what is now known as EECSNet, which is often described as the USMA Department of Electrical Engineering and Computer Science (EECS) cyber research network. Under the leadership of MAJ Kyle Moses, EECSNet became recognized by Academy IT leadership and was officially permitted to connect to the Internet. While still consisting primarily of equipment that was no longer useful to others, EECS department leadership would use gift funds to provide commercial Internet access and upgrade the more critical infrastructure. [12]

By 2018, EECSNet had been recognized by EECS leadership as a mission critical service and funding become more reliable and repeatable. Beginning with an upgrade to the server infrastructure and expanding storage through the addition of a SAN, EECSNet became capable of supporting a large cross section of the academic courses. Due to the virtualized nature of EECSNet, most of the issues and limitations discussed in the original IWAR paper can now be handled without adjusting any physical hardware. Cadets can have complete capture the flag environments built in a secure way at the click of a button. Courses will often spin up 200 machines in support of a lab or final exam.

Comparison

The modern day EECSNet, illustrated in Figure 2, is primarily a cluster of eight Dell R540 servers that are running as VMWare vCenter hosts with a total of 2.99 TB of RAM and nearly 447 GHz of computing capacity.

EECSNet has a 181 TB SAN, a 10 Gbps network backbone, and due to the generally lightweight nature of the machines, has the capacity to host more than 1,000 virtual machines. Its network infrastructure gives access to EECSNet throughout the EECS academic area and is accessible via VPN when cadets need to do work outside of the academic area. EECSNet has been recently recognized by the enterprise IT services and is present on an isolated VLAN within the Academy network. This means that EECSNet services can now be made available throughout the campus as unique usage and requirements are defined.

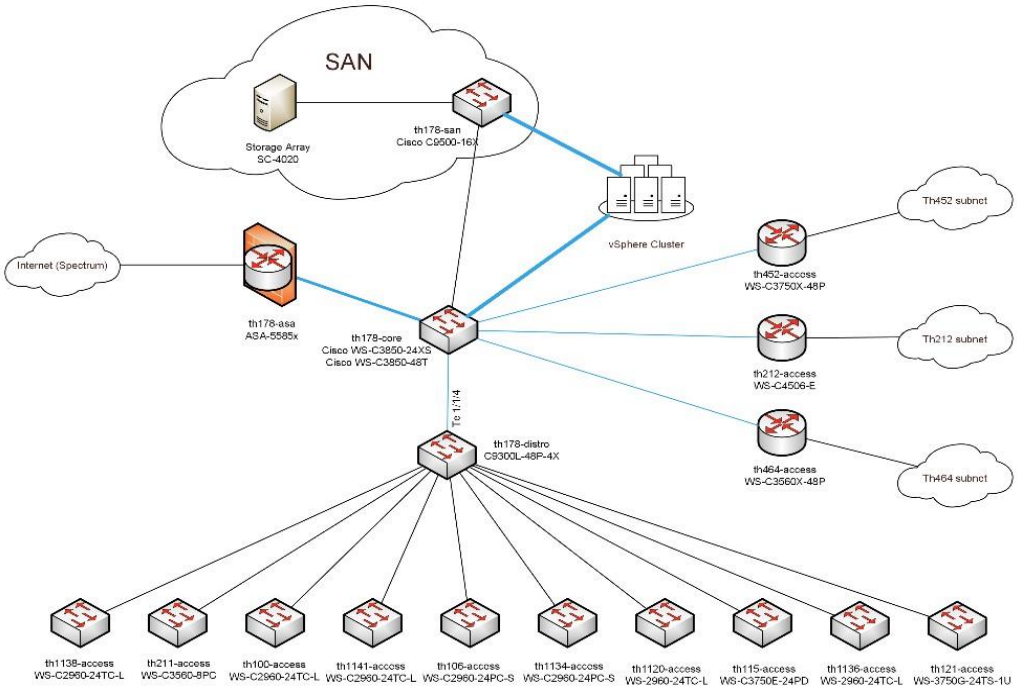

Figure 2: EECSNet diagram.

The move from a physical infrastructure to a virtual one gives faculty a level of flexibility that was never available previously. Solutions have been created that range from fully isolated and only accessible through a console to Internet connected and accessible from the public Internet. Virtual infrastructure also provides the ability to create unique machines for every student rather than requiring the sharing and/or reconfiguring of physical machines for each student. The ability to create a template virtual machine and script the creation of hundreds of machines means that the setup time required for a complex scenario is also significantly shortened.

Continuity

Surprisingly, despite the vast changes in the cyber environment since the inception of IWAR Range, many of the novel architectural decisions such as leveraging virtual machines and enabling attack, defense, and observers have endured at West Point and become ubiquitous. In the original paper[30], the authors describe four design criteria, "First, our design must allow minimal possibility of misuse or damage to other systems. Second, we had to make use of on-hand resources. Third, we had a very short time. Finally, we had to fit it into one classroom." EECSNet has learned to resolve these issues using more modern techniques than those described in the original design but with the same objective endstate.

To prevent misuse or damage to other systems, EECSNet leverages isolated Virtual Local Area Networks (VLANs). Depending on the specific scenario, those VLANs may be allowed controlled access to parts of the Internet, but in others are kept completely isolated. Accessing virtual machines in a completely isolated network is done using virtual consoles, which are accessible in a web browser. EECSNet has a long tradition of using on-hand resources and has only recently become a network that receives an annual budget for life-cycle replacement and expansion of capabilities. The short time criteria defined in the original IWAR Range design is managed using scripted lab generation. Using tools such as VMWare's PowerCLI or HashiCorp's TerraForm, faculty can create cyber research and contest infrastructure very quickly. Finally, EECSNet now consists of a single rack of hardware holding eight servers, two storage appliance devices, a firewall, and a core switch/router.

EECSNet ties its lineage back to the original IWAR Range and is now the gold standard for easily reconfigurable cyber ranges. Additionally, it was the inspiration behind a much larger IT transformation that has brought West Point IT services back in line with its peer institutions.

IWAR to WREN

Beginning in 2015, West Point started to realize that the mission of the Army to secure the Department of Defense Information Network (DoDIN) and the mission of West Point to educate cadets were at odds and that the IT infrastructure was lagging peer institutions. West Point needed IT services that were focused on education and allowed users the freedom and flexibility to use their computers as they wished. DoDIN had to be secured in such a way that connecting to it hindered West Point's mission and its ability to maintain higher education accreditations.

Leaders began a study to determine the best path forward for IT at West Point. The result was the most significant IT transformation every undertaken at West Point and the creation of the West Point Research and Education Network (WREN). The WREN is a cloud-first, education focused set of IT services that is on par with the best universities.

At the heart of the WREN is EECSNet and its predecessor, the IWAR Range. The freedom to conduct cyber research and education without IT infrastructure getting in the way is why IWAR was created in the first place. It is what kept the ideas behind the IWAR Range alive and turned it into EECSNet, and it was the catalyst for the creation of the WREN. In addition to the ideas behind the IWAR Range and EECSNet, the engineers that designed, built, and secured the WREN were the same people who honed their skills designing, building, operating, and maintaining EECSNet.

Defense Cyber Education Future

The urgency, necessity, and impact of cyber education is apparent and widespread from the ranges and courses to the cities and international influences. The U.S. military emphasis on information and cyberspace has soared in the past few years with: (1) the recognition that Cyberspace is the fifth domain of warfare (alongside Land, Sea, Air, and Space), (2) the promotion of the U.S. Cyber Command to Combatant Command status, and (3) most recently the elevation of Information as the seventh joint function (The Joint Functions are: C2, intelligence, fires, movement and maneuver, protection, sustainment, and information.) [14:III–1]. Sun Tzu, the Chinese strategist, wrote 2,500 years ago, "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting." [32:17]

Recent elections serve to highlight the importance of cyber-enabled international information power and foreign malign influence in cyberspace below the level of armed conflict.[29]. Cyber ranges and curricula at our academies and war colleges will continue to evolve. Like EECS ITOC faculty from twenty years ago, the West Point CRC and ACI as well as the NDU CIC continue to improve cyber defense and to inform the "emerging dialogue on the direction, content, and techniques involved in cyber education". [31]

About the Authors

Joseph H. Schafer

Professor and Associate Dean, College of Information & Cyberspace
National Defense University, Fort McNair, Washington, DC 20319
joseph.h.schafer.civ@ndu.edu

Christopher Morrell

Associate Professor and Cyber Science Program Director
Department of Electrical Engineering & Computer Science (EECS)
United States Military Academy, West Point, NY 10996
christopher.morrell@westpoint.edu

Raymond Blaine

Associate Professor and Director, Cyber Research Center, EECS
United States Military Academy, West Point, NY 10996
raymond.blaine@westpoint.edu

References

[1] ACI. 2018. *History Report Army Cyber Institute 2016-2017*. Army Cyber Institute, West Point, NY. https://cyber.army.mil/Portals/3/Documents/reports/History%20Report%20Army%20Cyber%20Institute%202016-2017.pdf?ver=2018-01-18-092852300

[2] ACI. 2022. Jack Voltaic. https://cyber.army.mil/Research/Jack-Voltaic/

[3] AFCEA. 2019. Lockheed is Assisting DOD with a National Cyber Range. *SIGNAL Magazine*. https://www.afcea.org/content/lockheed-assisting-dodnational-cyber-range

[4] @ArmyCyberInst. 2022. Cyber Defense Review. https://cyberdefensereview.army.mil/

[5] BBC. 2011. U.S. builds net for cyber war games. *BBC News*. https://www.bbc.com/news/technology-13807815

[6] CCSC. 2022. History | CCSC - Consortium for Computing Sciences in Colleges. http://www.ccsc.org/about-us/history/

[7] Ciro Rodriguez. 2010. *Recognizing the National Collegiate Cyber Defense Competition for its now five-year effort to promote cyber security curriculum in institutions of higher learning. (2010 - H.Res. 1244)*. https://www.govtrack.us/congress/bills/111/hres1244

[8] CRC. 2019. About the Cyber Research Center | United States Military Academy West Point. https://www.westpoint.edu/centers-andresearch/cyber-research-center/about

[9] David Raymond. 2022. Virginia Tech Faculty: David Raymond. https://security.vt.edu/content/security_vt_edu/en/about/faculty_staff/david_raymond.html

[10] Dan Farmer. 1995. SATAN (Security Administrator Tool for Analyzing Networks). http://www.fish2.com/satan/

[11] Neil Gaudreau and Jeffrey Combs. 2012. DoD Cyber Range. *CHIPS Magazine Vol. XXX Issue III*, 22–26.

[12] David P Harvie, Jason R Cody, Christopher Morrell, and Tanya T Estes. 2019. Using Virtual Machines to Enhance the Educational Experience in an Introductory Computing Course. (2019), 5. DOI:https://doi.org/10/ghnsvx

[13] IAWS. 2007. Information Assurance and Security Workshop 2007. In *Proceedings of the 8th IEEE SMC Information Assurance Workshop*, IEEE Systems, Man, and Cybernetics Society, West Point, New York., 385. http://ieeexplore.ieee.org/servlet/opac?punumber=4267526

[14] JCS. 2017. *Joint Publication 3-0, Joint Operations*. Joint Chiefs of Staff, The Pentagon. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

[15] Jeremy Bunkley. 2015. Army Cyber Institute hosts summit, builds civilian/military cyber partnership. https://www.army.mil/article/148685/army_cyber_institute_hosts_summit_builds_civilianmilitary_cyber_partnership

[16] Kopidion LLC. 2022. About Kopidion. *Kopidion*.

http://www.kopidion.com/about-us.html

[17] MCPA. 2020. Lockdown Lunch & Learn (3L). *Military Cyber Professional Association*. https://public.milcyber.org/activities/3l [18] Jeff Moss. 2007. The Story of DEF CON. https://www.americanrhetoric.com/speeches/jeffmossdefconstory.htm

[19] B. E. Mullins, T. H. Lacey, R. F. Mills, J. E. Trechter, and S. D. Bass. 2007. How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. *IEEE Security & Privacy* 5, 5 (September 2007), 40–49. DOI:https://doi.org/10/fsqmxr

[20] NDU CIC. 2020. *Cyber Beacon 2020. Disruption in an Era of Great Power Competition: Pandemic, Infodemic, Space, Cyberspace, and Beyond*. National Defense University, College of Information and Cyberspace, Fort McNair, DC. https://cic.ndu.edu/cyberbeacon/

[21] NECCDL. 2020. Past Winners. *Northeast Collegiate Cyber Defense Competition*. https://neccdl.org/history/sub1/

[22] NSA. 1999. *NSA Designates First Centers Of Academic Excellence in Information Assurance Education*. National Security Agency (NSA). https://www.nsa.gov/news-features/press-room/Article/1636090/nsadesignates-first-centers-of-academic-excellence-in-information-assuranceed/

[23] NSA. 2000. *NSA Announces Centers of Academic Excellence in Information Assurance Education for the Year 2000*. National Security Agency (NSA). https://www.nsa.gov/news-features/press-room/Article/1638982/nsaannounces-centers-of-academic-excellence-in-information-assuranceeducation/

[24] NSA. 2001. *NSA Announces the Designation of Centers of Academic Excellence in Information Assurance Education*. National Security Agency (NSA). https://www.nsa.gov/news-features/press-room/Article/1637330/nsaannounces-the-designation-of-centers-of-academic-excellence-ininformation/

[25] NSA. 2022. National Security Agency/Central Security Service > Cybersecurity > NSA Cyber Exercise. https://www.nsa.gov/Cybersecurity/NSA-Cyber-Exercise/

[26] NSA. The Inaugural NSA Cyber Exercise, former Cyber Defense Exercise, brings new cyber competition to U.S. Service Academy Cadets and Midshipmen. *National Security Agency / Central Security Service*. https://www.nsa.gov/News-Features/Feature-Stories/ArticleView/Article/1625583/the-inaugural-nsa-cyber-exercise-former-cyberdefense-exercise-brings-new-cyber/

[27] Steve Ranger. 2019. Cybersecurity: This giant wargame is preparing for the next big election hack. *ZDNet*. https://www.zdnet.com/article/cybersecuritythis-giant-wargame-is-preparing-for-the-next-big-election-hack/

[28] Matt Richtel. 1998. Hacker Group Says Program Can Exploit Microsoft Security Hole. *The New York Times*. https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html

[29] Joseph Hughes Schafer. 2020. International Information Power and Foreign Malign Influence in Cyberspace. In *Proceedings of the 15th International*

Conference on Cyber Warfare and Security, Academic Conferences and Publishing International Limited, Old Dominion University, Norfolk, Virginia, USA. https://www.academic-conferences.org/conferences/iccws

[30] Joseph Hughes Schafer, Daniel Joseph Ragsdale, John R. Surdu, and Curtis Arthur Carver Jr. 2001. The IWAR Range: A Laboratory for Undergraduate Information Assurance Education [Information Warfare Analysis and Research]. *The Journal of Computing in Small Colleges* 16, 4 (May 2001), 223–232.

[31] Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor. 2015. Cyber Education: A Multi-Level, Multi-Discipline Approach. In *Proceedings of the 16th Annual Conference on Information Technology Education - SIGITE '15*, ACM Press, Chicago, Illinois, USA, 43–47. DOI:https://doi.org/10/ghns4t

[32] Sun Tzu. 1910. *On the Art of War*. The British Museum, London. http://classics.mit.edu/Tzu/artwar.html

[33] TAMU. 2022. About Texas A&M Cybersecurity Center. https://cybersecurity.tamu.edu/about-us/

[34] Teresa M. Takai. 2014. *DoDI 8500.01 Cybersecurity*. DoD CIO, The Pentagon. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

[35] U.S. Cyber Command Public Affairs. 2020. During global pandemic, USCYBERCOM trains virtually to defend networks, protect nation. *U.S. Cyber Command*. https://www.cybercom.mil/Media/News/Article/2227651/during-globalpandemic-uscybercom-trains-virtually-to-defend-networks-protect-n/

[36] vulc@n of DDTek. 2012. DEF CON® Hacking Conference - CTF History. https://www.defcon.org/html/links/dc-ctf-history.html