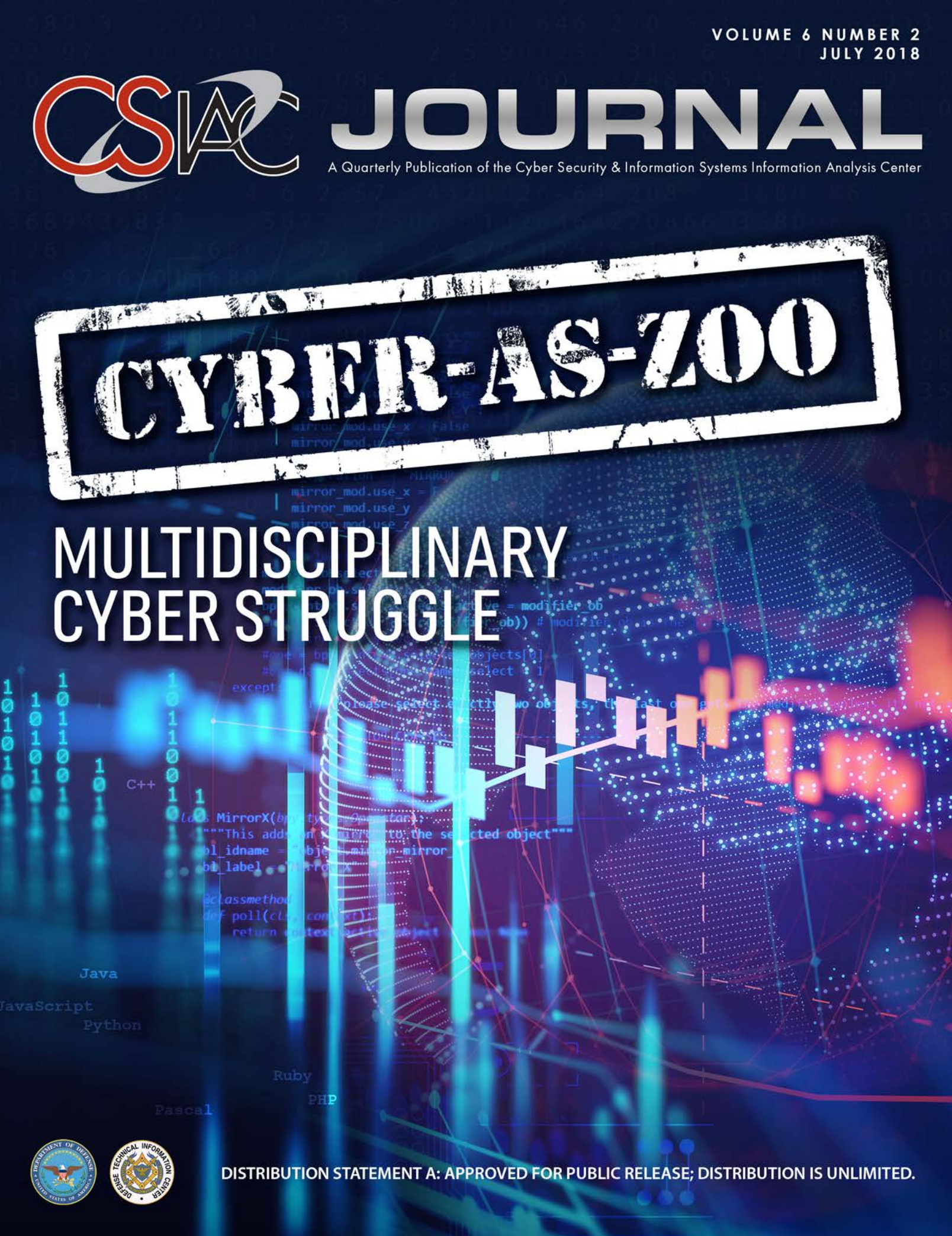
VOLUME 6 NUMBER 2
JULY 2018

CSIAC JOURNAL

A Quarterly Publication of the Cyber Security & Information Systems Information Analysis Center

CYBER-AS-ZOO

MULTIDISCIPLINARY CYBER STRUGGLE



CSIAC

Cyber Security & Information Systems
Information Analysis Center

ABOUT THE CSIAC

As one of three DoD Information Analysis Centers (IACs), sponsored by the Defense Technical Information Center (DTIC), CSIAC is the Center of Excellence in Cyber Security and Information Systems. CSIAC fulfills the Scientific and Technical Information (STI) needs of the Research and Development (R&D) and acquisition communities. This is accomplished by providing access to the vast knowledge repositories of existing STI as well as conducting novel core analysis tasks (CATs) to address current, customer focused technological shortfalls.

OUR MISSION

CSIAC is chartered to leverage the best practices and expertise from government, industry, and academia in order to promote technology domain awareness and solve the most critically challenging scientific and technical (S&T) problems in the following areas:

- Cybersecurity and Information Assurance
- Software Engineering
- Modeling and Simulation
- Knowledge Management/Information Sharing

The primary activities focus on the collection, analysis, synthesis, processing, production and dissemination of Scientific and Technical Information (STI).

OUR VISION

The goal of CSIAC is to facilitate the advancement of technological innovations and developments. This is achieved by conducting gap analyses and proactively performing research efforts to fill the voids in the knowledge bases that are vital to our nation. CSIAC provides access to a wealth of STI along with expert guidance in order to improve our strategic capabilities.

WHAT WE OFFER

We provide expert technical advice and assistance to our user community. CSIAC is a competitively procured, single award contract. The CSIAC contract vehicle has Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements.

Custom solutions are delivered by executing user defined and funded CAT projects.

CORE SERVICES

- Technical Inquiries: up to 4 hours free
- Extended Inquiries: 5 - 24 hours
- Search and Summary Inquiries
- STI Searches of DTIC and other repositories
- Workshops and Training Classes
- Subject Matter Expert (SME) Registry and Referrals
- Risk Management Framework (RMF) Assessment & Authorization (A&A) Assistance and Training
- Community of Interest (COI) and Practice Support
- Document Hosting and Blog Spaces
- Agile & Responsive Solutions to emerging trends/threats

PRODUCTS

- State-of-the-Art Reports (SOARs)
- Technical Journals (Quarterly)
- Cybersecurity Digest (Semimonthly)
- RMF A&A Information
- Critical Reviews and Technology Assessments (CR/TAs)
- Analytical Tools and Techniques
- Webinars & Podcasts
- Handbooks and Data Books
- DoD Cybersecurity Policy Chart

CORE ANALYSIS TASKS (CATS)

- Customer tailored R&D efforts performed to solve specific user defined problems
- Funded Studies - $1M ceiling
- Duration - 12 month maximum
- Lead time - on contract within as few as 6-8 weeks

CONTACT INFORMATION

266 Genesee Street
Utica, NY 13502

1 (800) 214-7921

info@csiac.org

/DoD_CSIAC
/CSIAC
/CSIAC

ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

ABOUT THIS PUBLICATION

The Journal of Cyber Security and Information Systems is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY.

ARTICLE REPRODUCTION

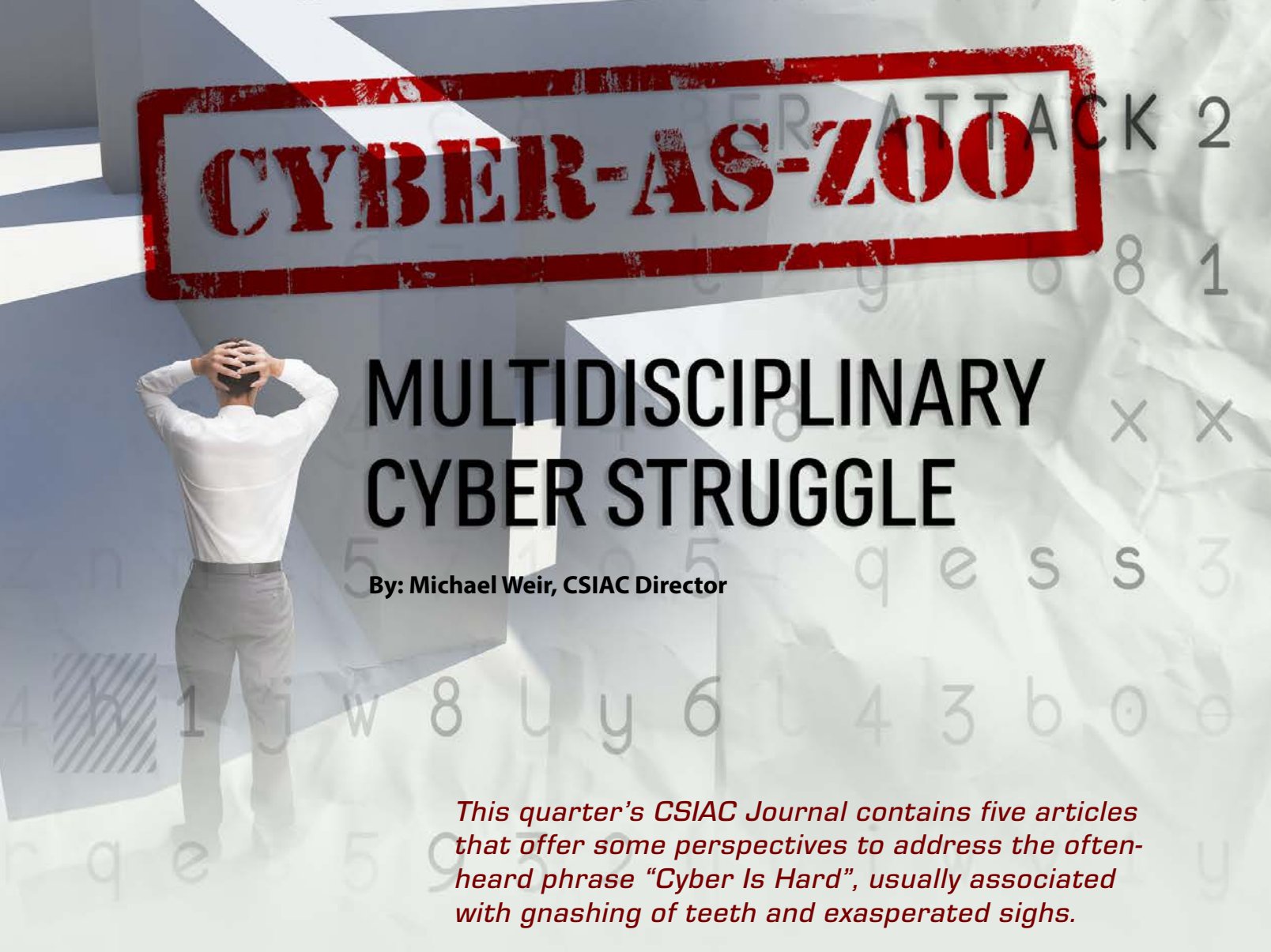
Cyber Security and Information Systems
266 Genesee Street
Utica, NY 13502

Phone: 800-214-7921
Fax: 315-732-3261
E-mail: info@csiac.org

An archive of past newsletters is available at **https://www.csiac.org/journal/.**

Journal of Cyber Security and Information Systems

Cyber-as-Zoo: Multidisciplinary Cyber Struggle



MULTIDISCIPLINARY CYBER STRUGGLE

By: Michael Weir, CSIAC Director

This quarter's CSIAC Journal contains five articles that offer some perspectives to address the often-heard phrase "Cyber Is Hard", usually associated with gnashing of teeth and exasperated sighs.

In particular, how can the Department of Defense deliver new concepts across the train/exercise/execute spectrum to provision cyber capabilities that can effectively address the rapidly changing world of cyber. To call cyber "multi-faceted" is too simple. Compared to the standard observation about near-sighted people observing an elephant in the room (everyone sees an aspect of the elephant, but nobody can see the whole animal), cyber is more like a zoo of animals in a room and the people are trying to find a single cage to put them in by collaborating on what their specific animals are like. Common ground is hard to find. Effectively moving forward involves smart people addressing as much as they can in their domain, while collaborating amongst themselves to share vocabulary and discover any possible higher-level common threads to help tie things together. The articles following cover many ideas and perspectives for the "cyber-as-zoo" we find ourselves in. The way ahead, unsurprisingly, is to maintain our focus on models and pragmatic demonstrations of practical aspects of cyber, while maintaining a dialogue and collaboration across domains. Over time, that approach will build a cyber terrain much like the modern equivalent of zoos, without cages – larger spaces, effective partitions, shared interactions where reasonable, higher-level understanding of relationships between domains.

The first article from Dr. Jamie Acosta, et al, from the Army Research Laboratory Center for Cyber Analysis and Assessment and the University of Texas at El Paso delves into the many aspects of training in the cyber domain, and the steps they have taken collaboratively across many tools, participants and goals to provide effective workshops that train/test/analyze cyber professionals at different levels. Identified early in that article is a specific observation that real network traffic of interest is very, very difficult to come by in the training domain. Real-world cyber defenders (organizationally and personally) are very hesitant to reveal full details about their defenses, problems, or actions (specific configuration of tools, actual threats, network traffic, etc.) – and for perfectly good reason. Unlike describing kinetic and physical battles that have occurred (… flanking maneuver, or flanking

manoeuvre is a movement of an armed force around a flank to achieve an advantageous position over an enemy **…), a cyber event is valid and actionable far beyond the physical space/time in which it first occurs. The authors then provide insight into their approach to making a positive impact on cyber professionals by integrating multiple tools into an emulation/simulation environment. They give specific instances of training objectives, components, and results that show us a realistic path to building better cyber professionals.

The second article is a thought article about standardization of cyber professional qualifications. Dr. Christopher Seedyk from U.S. Army Research Laboratory identifies a difficult problem to solve - how do you reconcile high-level, slow-moving standards at a policy level with fast-moving execution of cyber activities in an incredibly dynamic cyber-world in terms of qualification standards? Both ends of the spectrum are valid. Standards across large organizations are best formulated for long-term strategies across the work force. Effective execution of cyber actions requires up-to-date skills and understanding to keep up with patches, malware, zer0-days, etc. Chris leverages a Department of the Navy (DoN) personnel qualification standard to hypothesize an approach to connecting the general to the specific with appropriate update epochs to provide a possible path toward realistic cybersecurity competency assessment that supports the Department.

Artificial Intelligence (AI) integration into cyber operations will continue to grow, resulting in a need to integrate human and artificial "professionals" into teams. The best expected future will be teams of assets that share information between them to develop and execute the best actions to fulfill a military objective. It would not be difficult to hypothesize a scenario unfolding where a human team member expresses significant emotional aspects to their thoughts and actions. To bring some of the basic ideas of AI into this scenario, in particular the components at the Artificial Neural Networks (ANN) level, into better focus across readers of different backgrounds and domains, we asked Erik Wemlinger who is a Senior Data Scientist at Syracuse Research Corporation (SRC) to give some background and identify some of the knowledge management aspects of ANNs and intelligent emotion and sentiment analysis that could impact us in a future interaction environment that includes sharing ideas, knowledge, data, and decisions.

Moving from training and qualification, toward exercises and mission execution, Dr. David "Fuzzy" Wells and Derek Bryan from the United States Pacific Command (USPACOM) update progress on the Cyber Operational Architecture Training System (COATS), a long-term High-Level Task sponsored through the Defense Modeling and Simulation Coordination Office (DMSCO). Over the last four years, COATS has been a very pragmatic exercise enabler, combining historically difficult objectives of both the kinetic and physical and the cyber and logical domains. The authors identify with specificity the roadblocks they have encountered and addressed along the way, along with ideas and recommendations for what comes next.

In the final article for this journal Giorgio Bertoli and Stephen Raio from the United States Army Communications-Electronics Research, Development and Engineering Center which tackles pragmatic execution of cyber missions under the popularly cited context of "Key Cyber Terrain." This article is the best representation of the "cyber-as-zoo" problem covered earlier. It is absolutely natural for any given domain expert to view cyber in terms and concepts derived from their vocabulary; domain-restricted models are part and parcel of how we as humans solve problems. It is also almost impossible to come to a collaborative cyber capability with that approach.

A COLLABORA

for Cybersecurity Research, Analy

By: Dr. Jaime C. Acostaa, Salamah Salamahb, Edgar Padillab, Monika Akbarb, Alexander,
U.S. Army Research Laboratory, University of Texas at El Paso

TION PIPELINE

ytics, and Tools

Cybersecurity Data Gap

Network and host-based sensors collect data that are foundational for current-day cybersecurity technologies such as intrusion detection and prevention systems. However, for cybersecurity incidents, these data only tell a part of the story. Lacking are the data from the inside view (or attacker perspective), including specific attacker actions, tools used, and strategies. Availability of such data will lead to technologies that provide decision support, perform automated security testing, and strengthened intrusion detection systems.

Technologies for Data Acquisition

Cybersecurity-related incidents in our world today are an unfortunate, yet common, occurrence. Networks typically collect activity traces during such incidents. As examples, Microsoft provides an application programming interface (API) for Windows Event Log, Windows Event Tracing, and also a suite of tools to collect and view these data [1]. Linux and Macintosh operating systems (Mac OS) have similar mechanisms with, for example, syslog, logger, and Snoopy [2]. Wireshark, tshark, and tcpdump are widely used sniffers for collecting network traffic. Analysis engines such as the Bro, Snort, Open Source HIDS Security (OSSEC), and HBSS Intrusion Detection Systems (IDS) monitor data and issue alerts for potentially malicious activities [3]. Very often, however, such data are not shared among the cybersecurity community due to its sensitivity. Most cyber datasets available to the public are collected during Capture The Flag competitions (CTF). DEFCON [4] has hosted yearly CTF events for over 20 years. After each event, the tools, data, write-ups, and source code for the challenges and CTF engine are released to the public. The International CTF (iCTF) [5] has held CTF events at an international scope over the past 12 years. However, datasets collected through these events have limitations; they mostly consist of network data alone, the data are mixed (participants are on the same network), and in many of these events, the objectives are not necessarily representative of real-world scenarios and instead focus on the competitive, game aspect in the assigned tasks.

For this reason, researchers tend to use emulation and simulation engines to design realistic and mock-up cybersecurity scenarios for collecting data and testing new concepts. For example, the Common Open Research Emulator (CORE) [6] is capable of emulating hosts and network devices at the network layer and above. These nodes can also install and execute services and applications. CORE supports Hardware-In-the-Loop (HIL) and is easily configurable and extensible, which makes it a good platform for creating scenarios that can be migrated to other systems. The Extendable Mobile Ad-hoc Network Emulator (EMANE) [7] can be used separately or alongside CORE to provide emulation for the physical and data link layer. These technologies are very well suited for providing flexible, efficient, and simultaneous experimentation environments. However, some additional key features must be implemented for comprehensive and large-scale data acquisition (including the inside, attacker, view).

Driving Facilities

The Center for Cyber Analysis and Assessment (CCAA), located at the University of Texas at El Paso (UTEP), an Army Research Lab (ARL)-South Satellite campus, was established to tackle these issues. The center brings together government, industry, and academic partners to partake in and develop hands-on workshops that help to understand and develop solutions for real-world technology gaps and research questions. The Cybersecurity through Workshops, Analysis, and Research (CyWAR) laboratory is a collaborative working area that offers shared office space for collaborators.

The successful collaboration between ARL and UTEP is primarily fueled through in-kind contributions. The Software Engineering courses (both at the undergraduate and graduate level) build tools and techniques to tackle real-world, current-day, problems. UTEP Scholarship

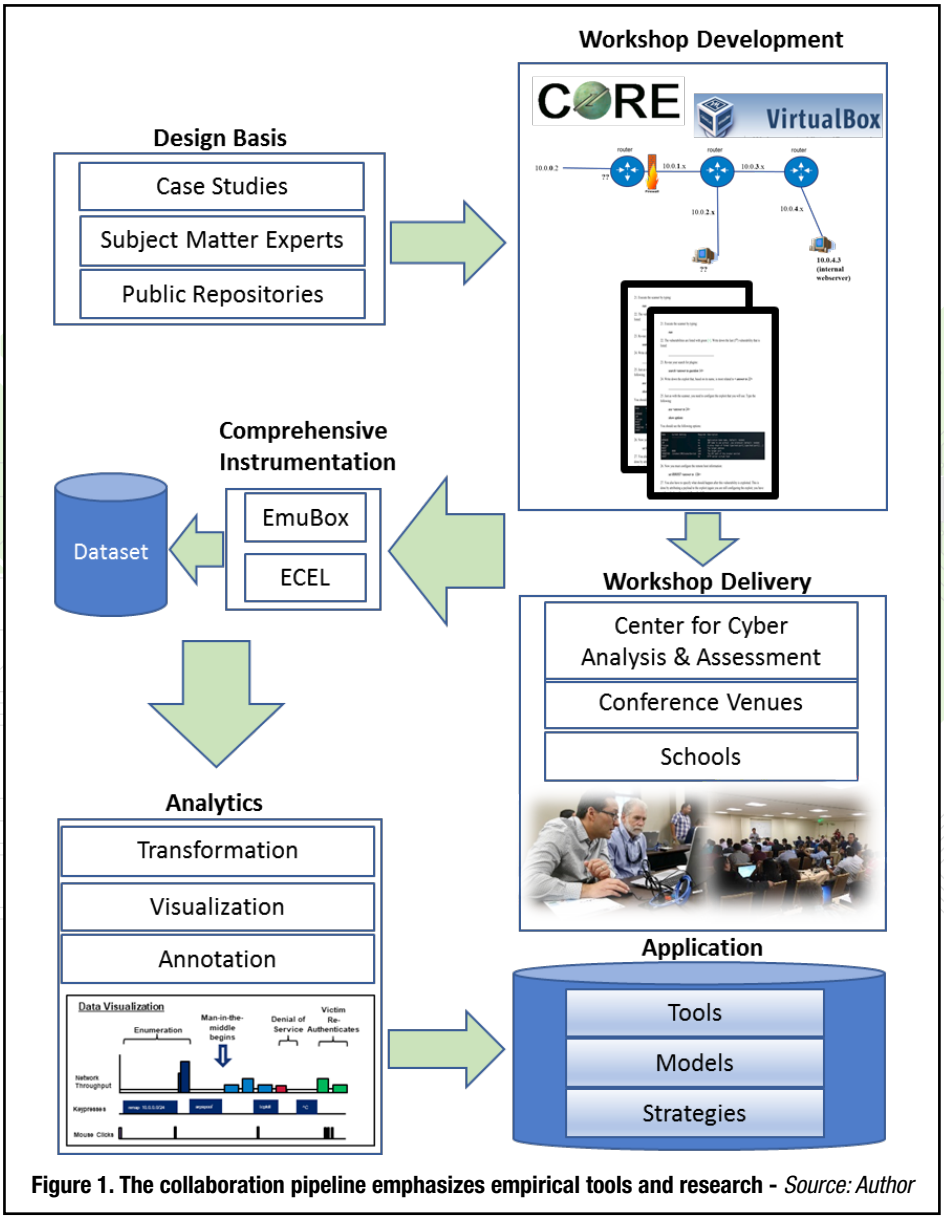


Figure 1. The collaboration pipeline emphasizes empirical tools and research - *Source: Author*

for service (SFS) students at the Master and Doctoral levels refine and tailor the developed software for use in cybersecurity research. Collaboratively developed coursework and workshops help to attract students to UTEP's cybersecurity programs and to satisfy engagement requirements for University designations such as the National Security Agency (NSA) Center of Academic Excellence (CAE) in both Cyber Defense and Cyber Operations.

Collaboration Pipeline

ARL-UTEP collaborative interactions form a pipeline where critical emphasis lies on empirical research and tools that coincide with the fast-paced field of cybersecurity (see Figure 1).

Design Basis and Workshop Development

The development of hands-on cybersecurity workshops involves students from ARL researchers and other experts investigating publicly known cybersecurity incidents, tools, and vulnerabilities. This involves consulting experts in specific technical areas and understanding current technologies and their weaknesses. A scenario outline, that describes the steps an attacker may take to compromise the system is documented as an exercise for workshop participants. This document includes the goals and outcomes for each phase in the exercise. After being reviewed by the ARL-South group, the network topology is developed using the CORE and VirtualBox. Any custom Virtual Machines (VMs), e.g., a Windows 7 machine vulnerable to the WannaCry ransomware, are configured separately and connected to CORE through its HIL feature.

A typical workshop's duration is between one and three hours. To accommodate multiple skill levels, each workshop consists of a regular challenge and an advanced challenge. The advanced challenge encourages participants to research external resources and leverage the knowledge gained during the regular challenge. The following are the sample steps involved with two such workshops.

Workshop: Pivoting and Exploitation

In this workshop, participants are located on the Internet and must gain access to an email server that resides in an Intranet. The Intranet has a host that is running a publicly accessible and vulnerable JBoss service. Participants are given a document that was apparently found while dumpster diving. It describes several subnetworks in the Intranet, including IP addresses and subnet masks.

Participants complete the following tasks: 1) find the IP address of the node serving the JBoss service by scanning the Intranet, 2) use Metasploit to identify and exploit a vulnerability in the JBoss service and to run a Meterpreter session, 3) configure the compromised node as a pivot by configuring routing and using a socks4a proxy, and 4) access the internal email server using the browser.

Workshop: Route Hijacking

In this workshop, participants lack prior knowledge about the network. They are connected to a routing gateway that is using the Routing Information Protocol (RIP) for dynamic routing.

Participants complete the following tasks: 1) use Wireshark to view the routing network packets and identify all subnetworks, 2) spoof a plaintext authentication web page running on a remote host, 3) host the spoofed web page, 4) use the Loki.py tool to advertise a false route to the web server, and 5) use Wireshark to retrieve user credentials.

Table 1 lists additional workshops that have been developed collaboratively between academia, government, and industry.

Workshop Delivery

Over the past two years, we have hosted over 15 workshops and hosted over 800 participants. While we primarily use the CCAA to host workshops for students and professionals, we have also conducted workshops at external venues including the Hispanic Engineer National Achievement Awards Corporation (HENAAC) Conference and the White Sands Missile Range Leaders New Mexico (LMN) event.

There are several ways to deliver workshops. If held outside of the Center, participants use their own computers; if held in the Center, or furnished laptops. In the former case, the only requirement is that laptops have remote desktop client software, such as Microsoft Remote Desktop or rdesktop (Linux). Workshops start with a presentation that describes background knowledge related to the security issue or incident. While most of the workshops target freshman

Table 1. Collaboratively developed workshops - *Source: Author*

Workshop Name	Description
WannaCry ransomware	Infect a Windows 7 machine, observe traffic, find and implement the kill switch so that the malware will no longer spread.
DEFCON challenges	Recreated qualifying challenges for the DEFCON capture-the-flag events.
Slow HTTP POST Denial of Service (DoS)	Understand the Slowloris DoS tool, recreate effects, and configure a web server for prevention.
Cross-site scripting	Identify weak JavaScript code and use it to obtain a victim's information and then fix the code vulnerability.
Bot malware forensics	Use volatility to identify and reverse engineering an infected process. Decode communication and obtain additional information from the bot master.
Watering hole	Scan and find a vulnerable HTTP File System service on a web server and then replace a legitimate file with a reverse shell. Afterwards, apply defense in depth to harden the system.
Reverse engineering	Use IDA Pro to find the password for an encrypted malware file.
Buffer overflow	Identify a weakness in an FTP server program and use Metasploit to generate shell code. Afterwards, apply defense in depth to harden the system.
ARP spoof	Understand the arpspoof tool in Kali Linux OS and then use it to eavesdrop on traffic. Afterwards, propose potential fixes.

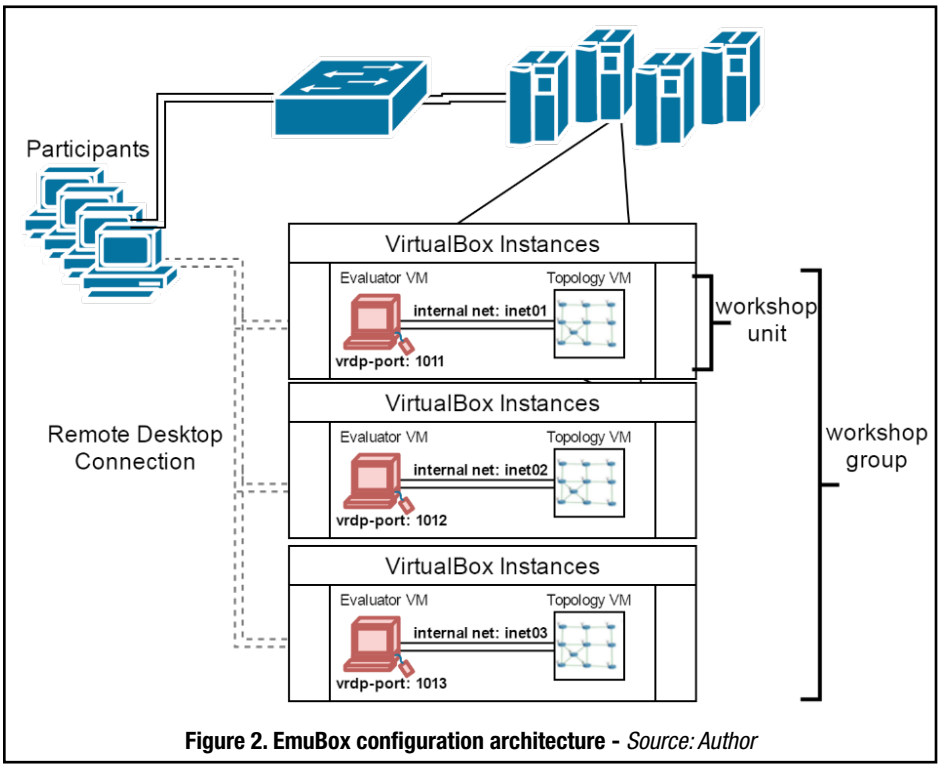


Figure 2. EmuBox configuration architecture - *Source: Author*

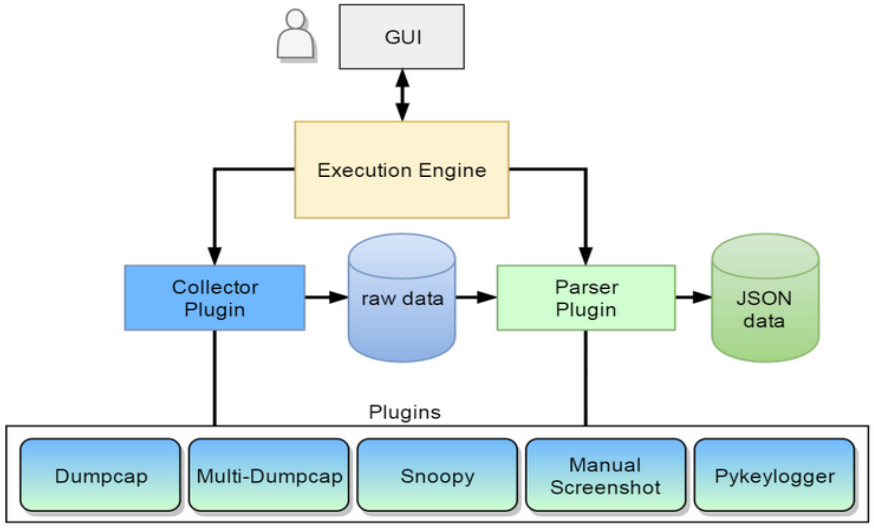


Figure 3. ECEL software architecture - *Source: Author*

to sophomore-level college students (e.g., WannaCry ransomware), a few are designed for cybersecurity professionals (e.g., the DEFCON challenge). To start the exercise, participants navigate to a webserver and then download and open a Remote Desktop Protocol connection (RDP) file.

If the workshop is used for training or awareness, participants are given an exercise handout that consists of fill-in-the-blank questions mixed with short explanations. During the exercise, the workshop developers and other aids answer questions and offer guidance. If used for testing, participants are given an objective and offered little or no guidance.

The Backend: Execution and Instrumentation Tools

Our pipeline uses two collaboratively developed tools. The Emulation Sandbox (EmuBox) is used to serving multiple simultaneous scenarios and the Evaluator-Centric and Extensible Logger (ECEL) is used for collecting data. Below is a description of each of these tools.

EmuBox

The EmuBox is a lightweight, open source testbed[1]. It is written in Python and has been tested on Windows 7+, Kali Linux 2016.1, 2016.2, and Ubuntu 14.04 LTE (32 and 64 bit). The EmuBox leverages VirtualBox and CORE to support mixed virtual/physical systems, virtual remote desktop connection (VRDP), and heterogeneous (e.g., mixed MANET and wired) networks.

The EmuBox can host up to 8 simultaneous participants on a laptop with an Intel i7 process and 16GB of memory. Figure 2 shows a setup using four computers to run the EmuBox and a network switch to connect participants to the internal virtual machines.

Scenario VMs are grouped into Workshop Units and Workshop Groups. Workshop Units contain the set of VMs that make up a single scenario. At least one of these VMs must have the virtual remote desktop protocol (VRDP) enabled (a feature of the VirtualBox extensions pack).

VirtualBox consumes VRDP data meaning that the traffic associated with the remote desktop connection is not visible within the VMs. A VM is used with CORE to construct the network topology. The topology may consist of Linux containers and Docker containers. Additionally, external hardware, such as a Controller Area Network (CAN bus), and other non-IP-based systems may be connected using HIL. Vulnerable systems, scripted actors (e.g., operators/defenders), and instrumentations may also be incorporated into the scenarios.

Network isolation is implemented using VirtualBox internal network adapters. After a Workshop Unit is configured, the machines are started and a snapshot is taken; this snapshot acts as a frozen image that preserves state and can be restored at a later time. For example, the snapshot may be taken after a user logs in and starts the sshd service or after all routes converge

1 Code can be found at: https://github.com/ARL-UTEP-OC/emubox

in the network topology. The EmuBox can also clone Workshop Units, or scenarios; adjusting VRDP ports and internal network adapter names so that each group is isolated and uniquely accessible by participants. Additionally, the EmuBox has a backend subsystem that provides a web frontend to show all available workshops and to restore VMs from snapshots once participants disconnect. See [8] for performance analysis.

ECEL

The ECEL is open source[2], written in Python, and is designed using a plugin architecture (see Figure 3). While the ECEL itself is cross-platform, some plugins are not, such as Snoopy, which is used for collecting system calls on Linux systems.

The ECEL's execution engine runs as a service that interfaces with backend functions for collection and parsing. Users may interact with the engine using the Graphical User Interface (GUI) or through a terminal window. The ECEL capabilities are easily extended through the implementation of collector and parser plugins. Collector plugins capture data from a resource such as tool output, system logs, or operating system hooks. Parser plugins read the captured data and transform it into a structured format. We have built plugins for network traffic (Dumpcap/Multi-Dumpcap), system calls (Snoopy), screenshots (Manual Screenshot) as well as keystrokes and mouse-clicks (Pykeylogger). Our parsers format data into JavaScript Object Notation (JSON) which is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types used during analysis. See [8] for an in-depth description of plugins. We walked through and captured a small dataset for the *route hijacking* and *pivoting & exploitation* workshops described earlier[3].

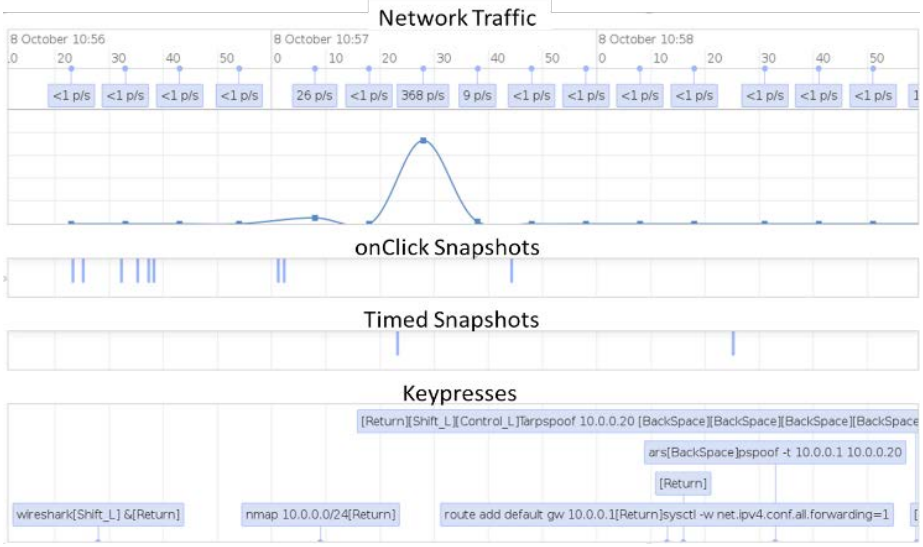


Figure 4. Timeline visualization screenshoot - *Source: Author*

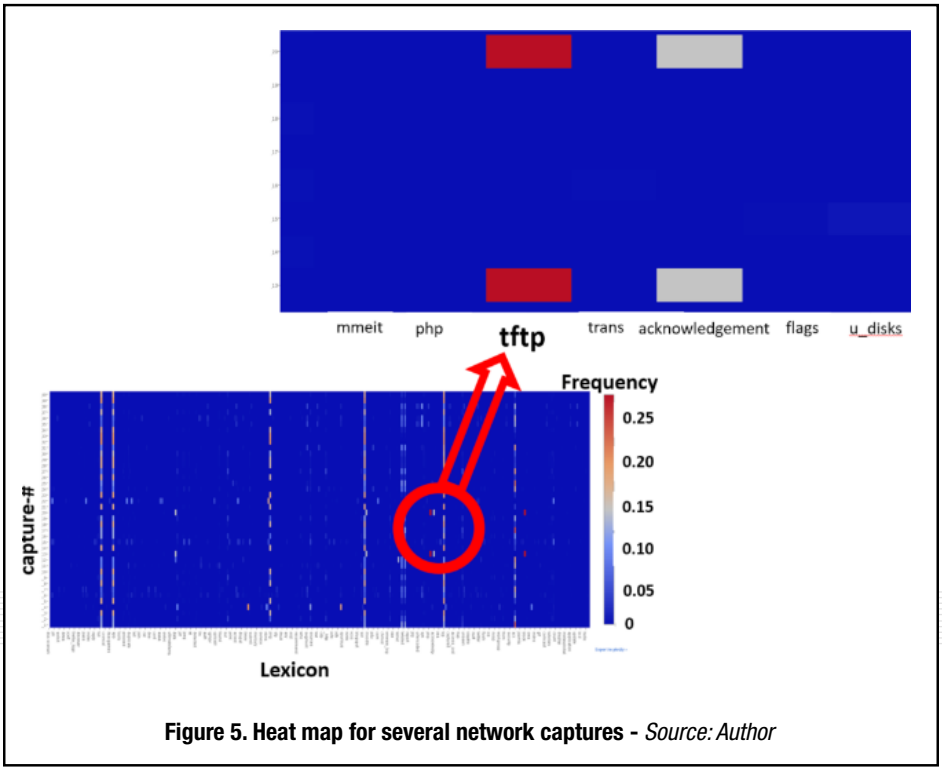


Figure 5. Heat map for several network captures - *Source: Author*

Data Analytics

To provide an efficient way to analyze data, there are several visualization tools. The timeline viewer, shown in Figure 4, is used for editing, annotating, and extracting portions of workshop-related data. This helps to map attacker actions to network traffic and to build models for decision support and attacker profiles.

The heat map viewer, shown in Figure 5, is used to identify similarity in network traffic across traffic captures and scenarios. This is used to improve intrusion detection systems and also to aid during security assessments (such as penetration testing) and to fine-tune and prune attack graphs, e.g., by assigning confidence metrics based on attacker profiles [9]. The heat map in Figure 5 shows two captures with high occurrences of the ***tftp*** lexicon (and, hence, the protocol).

Ongoing Research

The pipeline feeds into several research efforts that focus on the defensive and the testing aspect of security. The following are some examples.

2 Code can be found at: https://github.com/ARL-UTEP-OC/ecel

3 Datasets are available at: https://github.com/ARL-UTEP-OC/ecel-datasets

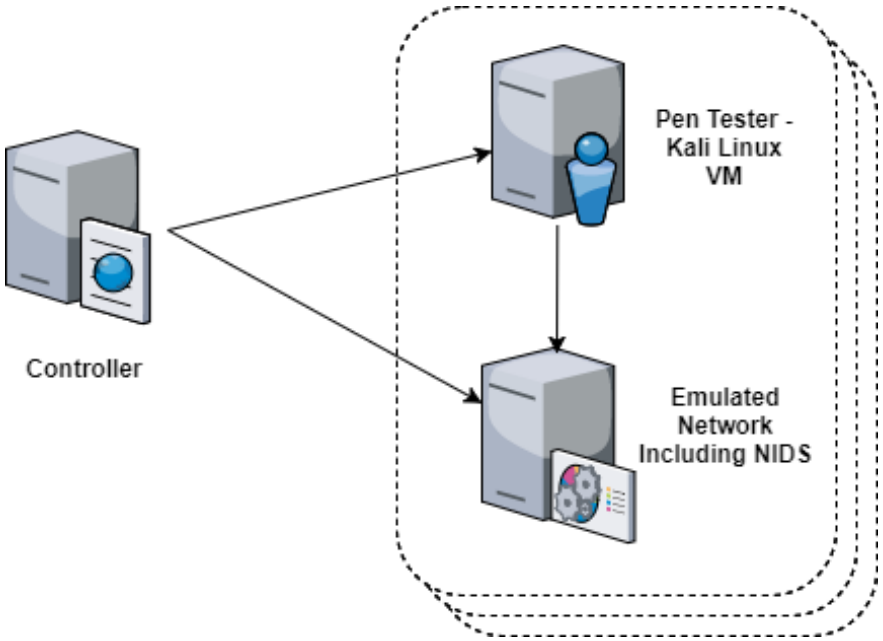


Figure 6. Our system gives researchers centralized control of several simultaneous experiments - *Source: Author*

Related to attack analysis and profiling, we employ temporal pattern mining and motif mining techniques to investigate the workshop data for detecting suspicious activities that frequently appear together in attacker's data streams. We study the correlation between network characteristics, network traffic, and system commands. We also conduct further studies to identify the best approach for modeling attacker's profile based on pre-intrusion and post-intrusion activities at the network and system level. In short, we are adding another dimension of training data (the inside view) to improve intrusion detections systems.

Another effort is attempting to extrapolate relationships between attacker actions and personality traits in relation to the dark triad (Machiavellianism, narcissism, and psychopathy). We have developed a system (see Figure 6 that leverages the EmuBox and the ECEL to analyze user network scanning and probing). Users complete a personality questionnaire and a workshop. We are attempting to identify correlations between the answers to the questionnaires and metrics related to actions, timing, and stealth. This work will help to predict attacker behavior in the early stages of an attack; probing and scanning are usually the first steps in an attack.

Regarding security testing, our work focuses on automated methodologies in the realm of protocol analysis and cybersecurity assessments. Using machine learning we are developing algorithms for automatic extraction of network protocol structures into a standardized format. We then use these structures to generate software templates that can communicate with non-IP protocols. Currently, the automated software generates ns-3 models, and Scapy which is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer [10].

We are also creating a decision support system for use by penetration testers (see Figure 7). Testers will be able to efficiently identify low-hanging fruit (i.e., findings that have been identified previously and are still unfixed) and to allocate more time and resources to test other, more complex, systems.

This system uses data collected during workshops with the ECEL and can also be trained to leverage in-house tools and techniques specific to an organization. Eventually, we will investigate the possibility of creating automated agents that execute a set of automated tasks; dependent on likelihood of success and collateral risk.

Conclusion

The relationship between ARL and UTEP has yielded many fruitful results. ARL has benefited by leveraging subject matter experts to cooperatively design and develop tools, conduct next-generation cybersecurity research, expand its overall capabilities, and also to attract and retain talent in the workforce. The University has strengthened its security program and outreach activities that have led to joint proposals and research grants among others. Students graduate with a firm understanding of cybersecurity concepts and issues augmented with practical experiences gained from working alongside experts in the field.

In the short term, we plan to make workshops accessible across the Internet by using virtual private network (VPN) which is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. and load balancing technologies. We will continue to expand our collaborative relationship and plan to reach out to other partners to develop and broaden our research focus.

REFERENCES

[1] Schauland, D., & Jacobs, D. (2016). Managing the Windows Event Log. In Troubleshooting Windows Server with PowerShell. Springer, 2016, pp. 17–33.

[2] Eriksen, M. A., & Skufca, B., "Snoopy logger," [Online]. Available: https://github.com/a2o/snoopy

[3] Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., & Payne, B. D. (2015). Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 48(1), 12.

[4] Nunes, E., Kulkarni, N., Shakarian, P., Ruef, A., & Little, J. (2016). Cyber-deception and attribution in capture-the-flag exercises. In Cyber Deception (pp. 151-167). Springer International Publishing.

[5] Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat, D. & Shoshitaishvili, Y., "Ten years of ictf: The good, the bad, and the ugly," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14). San Diego, CA: USENIX Association, 2014. [Online]. Available: https://www.usenix.org/conference/3gse14/summit-program/presentation/vigna

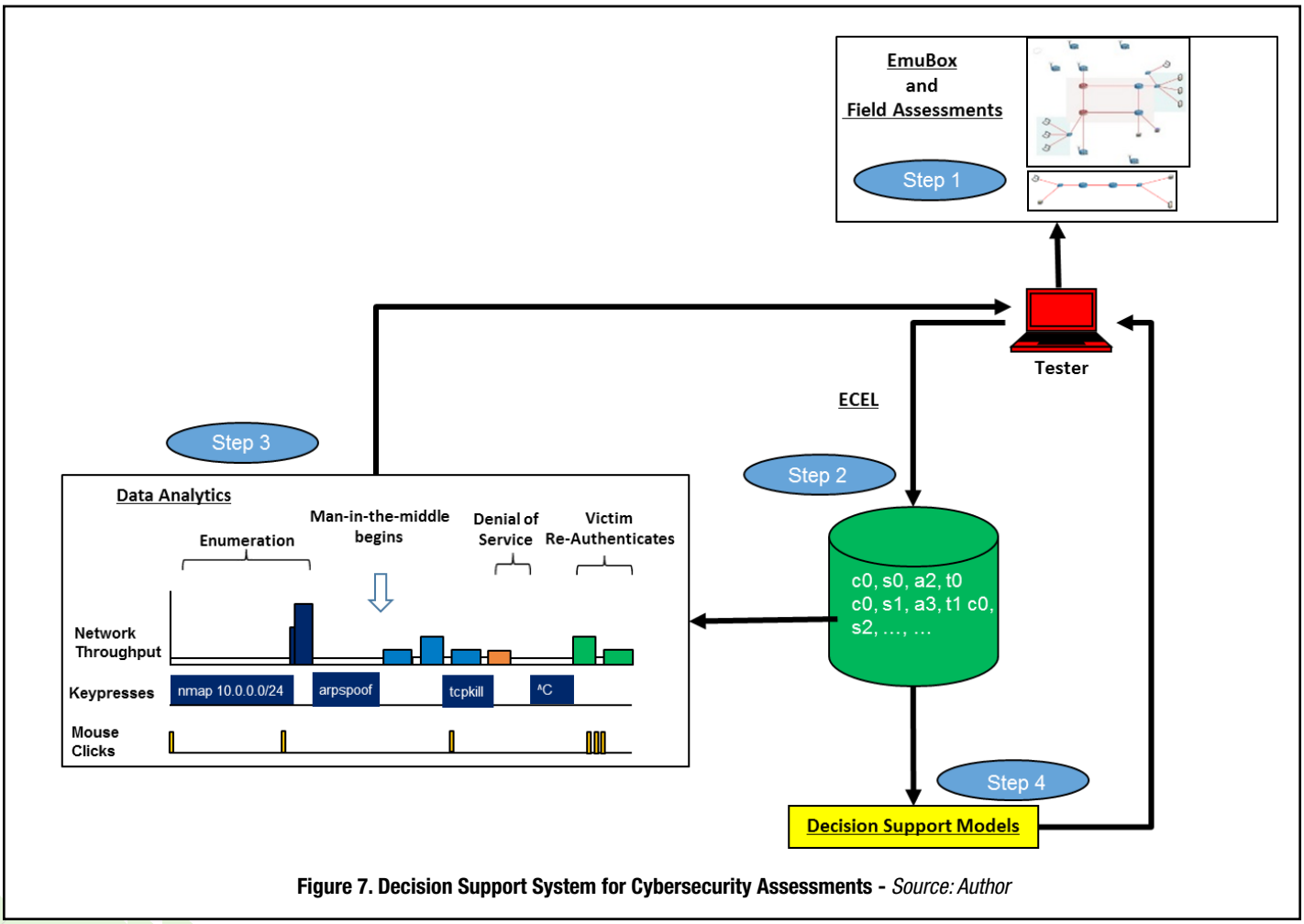


Figure 7. Decision Support System for Cybersecurity Assessments - *Source: Author*

[6] Ahrenholz, J., Danilov, C., Henderson, T. R., & Kim, J. H. (2008, November). CORE: A real-time network emulator. In Military Communications Conference, 2008. MILCOM 2008. IEEE (pp. 1-7). IEEE.

[7] Scott, L., Marcus, K., Hardy, R., & Chan, K. (2016, November). Exploring dependencies of networks of multi-genre network experiments. In Military Communications Conference, MILCOM 2016-2016 IEEE (pp. 576-581). IEEE.

[8] Acosta, J. C., McKee, J., Fielder, A., & Salamah, S. (2017, October). A Platform for Evaluator-Centric Cybersecurity Training and Data Acquisition. In Military Communications Conference, MILCOM 2017-2017 IEEE. IEEE.

[9] Acosta, J. C., Padilla, E., & Homer, J. (2016, November). Augmenting attack graphs to represent data link and network layer vulnerabilities. In Military Communications Conference, MILCOM 2016-2016 IEEE (pp. 1010-1015). IEEE.

[10] Acosta, J. C., & Estrada, P. (2017, May). A preliminary architecture for building communication software from traffic captures. In SPIE Defense+ Security (pp. 102060T-102060T). International Society for Optics and Photonics.

ABOUT THE AUTHORS

Jaime Acosta earned his Ph.D. degree from the University of Texas at El Paso. He works at the U.S. Army Research Laboratory and he directs the Center for Cyber Analysis and Assessment. His research interests include execution-based model generation, network security, and cybersecurity assessment methodologies.

Salamah Salamah is an Associate Professor in Computer Science at the University of Texas at El Paso (UTEP). He directs the school's Masters of Science in Software Engineering (MSSwE) program and the Cybersecurity through Workshops, Analysis, and Research (CyWAR) laboratory. His teaching and research interests include software engineering process, software quality assurance for safety-critical systems, formal methods in software development, and computer science and software engineering education.

Edgar Padilla is a Ph.D. student at the University of Texas at El Paso. He is also a systems programmer for the University's enterprise resource planning systems. His research interests include risk analysis and secure software architecture.

Monika Akbar is an Assistant Professor in Computer Science at the University of Texas at El Paso. Her research interests include information storage and retrieval, data and information management, data analytics, and cybersecurity.

Alexander Fielder received his M.S. degree in Computer Science from New Mexico State University. He has worked as a cyber analyst for the U.S. Army Research Laboratory for three years and holds several cybersecurity certifications including CISSP, CEH, and Security+.

CYBERSECURITY COMPETENCY ASSESSMENT

Using Augmented Qualification Standards

By: Dr. Christopher Seedyk

Determining the capabilities of cybersecurity personnel is essential to support the Department of Defense (DoD) Cyber Strategy.

The cyber ability of the DoD is contingent upon the continued high standard of performance of cybersecurity and computer network defense (CND) personnel. These personnel are all members of the DoD, the parent organization, but are dispersed in a wide variety of component (subordinate) organizations. Methods to assure a certain minimum level of competency, such as industry certifications and service component schools, can certify and qualify individual ability but are likely unable to qualify cyber individuals on the specific operations of component organizations. This article describes a framework for developing individual-centric and organization-specific qualification standards to augment existing qualification standards to assess the required cybersecurity skills that are unique or specific to component organizations.

Augmented Qualification Standards

Department-wide qualification and certification standards are necessary to support the DoD Cyber Security Strategy, and to ensure a consistent and standardized baseline for individual and organizational cybersecurity ability exists throughout the DoD [2]. However, when considering the specific operations and activities of component organization, there is a unique challenge. If standards take a generalized approach, then the standard can be applied to all component organizations of the parent organization but cannot address the unique requirements and nuances of these component organizations. If standards take a specific approach, then the standards can incorporate all of the requirements of each component organization, but the standard becomes time-consuming to develop, contains large portions of content that are not applicable to component organizations, and places an unnecessary burden on individuals participating in the qualification process [4].

To overcome these limitations, organizations can deploy augmented qualification standards that support the existing qualification requirements of the DoD while addressing additional organization-specific and individual-centric qualifiers. In doing so, the component organization satisfies both the parent organization requirements for a general baseline ability, and the organization-level requirements for tailored operations and capabilities. The DoD is positioned to understand the strategic requirements of its component organizations, but these individual component organizations are best poised to understand their own operational requirements and should design their qualifications accordingly [3]. To accomplish this, while ensuring that qualification standards remain relevant, organizations should strive to rapidly develop and deploy qualification standards for their operational personnel. In line with the current tradition of qualifying individuals, these standards should be individual-centric. This is partially realized in initiatives to develop job-based requirements, such as the US Navy's Job Qualification Requirements [1], but there is no defined emphasis on rapid development to maintain currency.

The Department of the Navy (DoN) implements a Personnel Qualification Standard (PQS) to certify a required minimum level of competency for individuals when performing certain job functions or tasks [5]. The structure of the Personnel Qualification Standard, as outlined in the *Personnel Qualification Standard Unit Coordinators Guide*, was used as the inspiration for the development of the Analyst Qualification Standard (AQS). To facilitate the rapid development and deployment of a qualification standard, the framework for the PQS was condensed to five sections encompassed the minimum necessary qualification tasks and knowledge.

Department-wide qualification and certification standards are necessary to support the DoD Cyber Security Strategy

Individual Qualification Standards Structure

Line Items and Qualifiers

Line items are specific pieces of knowledge or tasks that make up the required sections and content for a qualification standard. Line items in a qualification standard are identified and grouped into sections, and sections are further grouped into levels. When an individual demonstrates knowledge of a subject or the ability to perform a task, a qualified individual, known as the Qualifier, indicates completion of the line item with his signature. When all requisite line items have been completed and appropriately signed by a Qualifier, an individual has completed their qualification standard and obtained the necessary qualification [5].

Fundamentals Level (1000 Level)

Each qualification has fundamental and basic knowledge that is required to understand and perform certain duties. These pieces of knowledge are applied to other areas of the qualification, using the law of primacy, individuals first master the basics which are then applied and expanded upon throughout the qualification to ensure mastery of the material. The original framework from the DoN referred to these as the Fundamentals Section. The developed AQS framework embraced these as the Fundamentals (1000 Level) that contain the basic fundamentals of technical knowledge necessary to perform cybersecurity duties [5].

Systems Level (2000 Level)

In addition to fundamental knowledge, cybersecurity personnel require knowledge of the specific tools and systems used to perform and conduct cybersecurity activities [4]. To address these, the complex systems used in performance of duties are broken down into the most basic components, termed systems. This breakdown allows the content to be covered expediently with greater emphasis on the overall complex system. Ultimately, this knowledge is combined with fundamental knowledge, then synthesized and applied, to accomplish practical tasks duties. The original framework from the DoN referred to these as the Systems Section. The developed AQS framework embraced these as the Systems (2000 Level), which to contain tools, techniques, and methods necessary to perform cybersecurity duties [5].

Applications Level (3000 Level)

Individuals who are qualified to participate in component organization cybersecurity operations must be able to execute required practical tasks in accordance with DoD and component organization policies, procedures, and guidelines. This execution ability is necessary to demonstrate complete synthesis of fundamentals into the use of tools, techniques, and methods, and the application of this to perform real-word, practical tasks. As such, individuals must be able to perform required tasks in accordance with the requirements in the 1000 and 2000 Levels. The original framework from the

DoN referred to these as the Watchstation Section. The developed AQS framework embraced these as the Applications (3000 Level), which contain the execution of key operational tasks of the component organization and the application of 1000 and 2000 Levels skills to address scenarios and solve complex problems [5].

Final Qualification

Qualified cybersecurity personnel must discharge their duty and participate in operations in a consistent and reliable fashion. Piecemeal assessment of fundamentals—tools, techniques, and methods—and practical application are ideal for obtaining knowledge, but assessment of actual ability is best determined in a simulated or practical environment [5]. The original framework from the DoN referred to this as a Final Qualification that, at the discretion of a superior authority, consisted of recommendations from qualifiers, observation of duties, a written examination, or an oral board examination. The developed AQS framework embraced this verbatim as a Final Qualification and selected an oral board examination to assess viable knowledge and tangible practical application with the least amount of administrative burden or time requirements. During the oral board examination, a panel of three qualified individuals assess both the theoretical and practical knowledge of a candidate on any topic or content of the AQS in a formal, closed book session.

Analyst Qualification Standards Development Framework

The AQS Development Framework uses a three-phase process. First, requirements for qualification knowledge and practice are identified using four key organizational inputs. Second, the requirements are analyzed and categorized, and then used to create required line items. Finally, a comprehensive review and revision process is used to develop a final AQS for immediate and rapid deployment and distribution.

Development Methodology

Requirements Identification. Requirements were identified using four key component organizational inputs: (1) parent organization required certifications, (2) component organization policies and standards, (3) component organizational operations and procedures, and (4) component organization practitioner experiences and histories. Figure 1 illustrates these inputs, the AQS Levels the enumerated requirements map to, and the application of these into a resultant qualification standard.

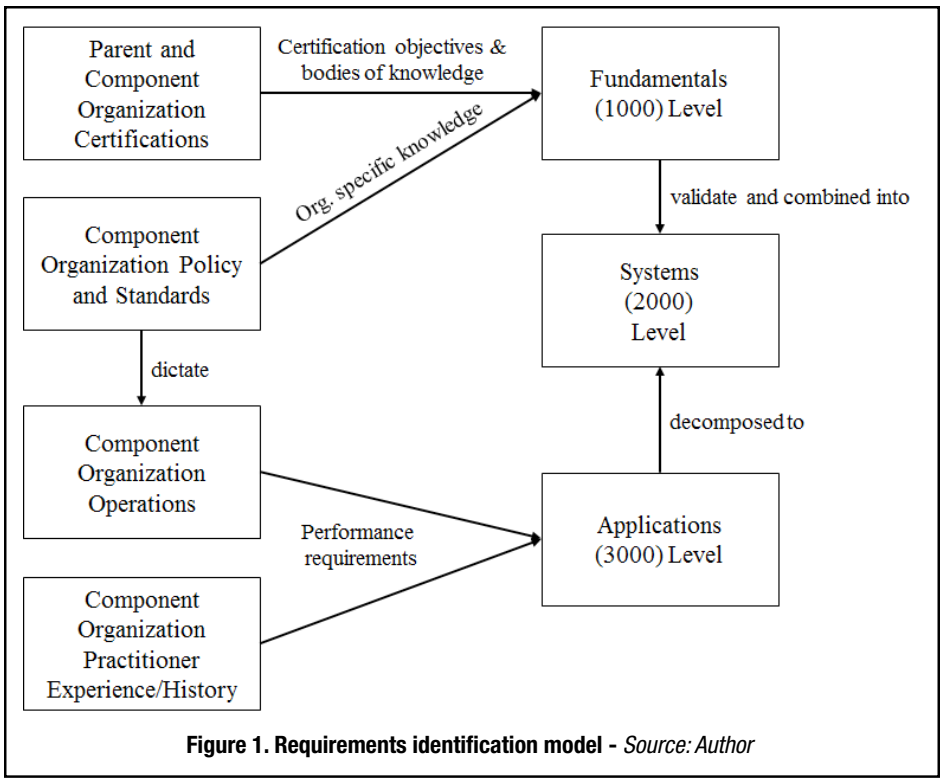


Figure 1. Requirements identification model - *Source: Author*

Using both parent organization and component organization mandatory certifications, requirements are enumerated from the certification objectives and common bodies of knowledge, using document analysis, to identify and generate requirements for the Fundamentals Level of the AQS. These represent specific knowledge needs, as identified by the parent organization, for individuals to perform job functions. Further document analysis on component organization policies and standards is used to enumerate component organization specific knowledge about operations, tools, techniques, and methods. This is also considered fundamental knowledge and is used to further populate requirements for the Fundamentals Level.

Thorough analysis of component organization operations, performance requirements for individuals can be enumerated using a combination of document analysis and active participant observation, and/or active participation. Document analysis of component organization operating procedures enumerates key tasks and steps required of individuals, while observation and/or active participation on events enumerates key activities that are performed. Each of these analyses creates performance requirements that populate the Applications Level of the AQS. Further, through the use of unstructured interviews with key component organization personnel, as identified by upper management, the resultant narrative can be subjected to a primitive coding process, using both priori and grounded

> assessment of actual ability is best determined in a simulated or practical environment

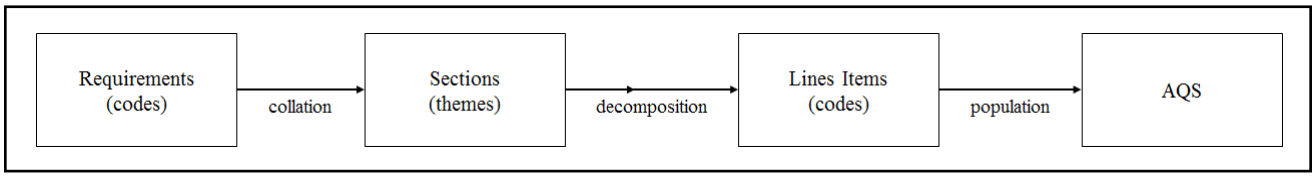


Figure 2. AQS construction model - *Source: Author*

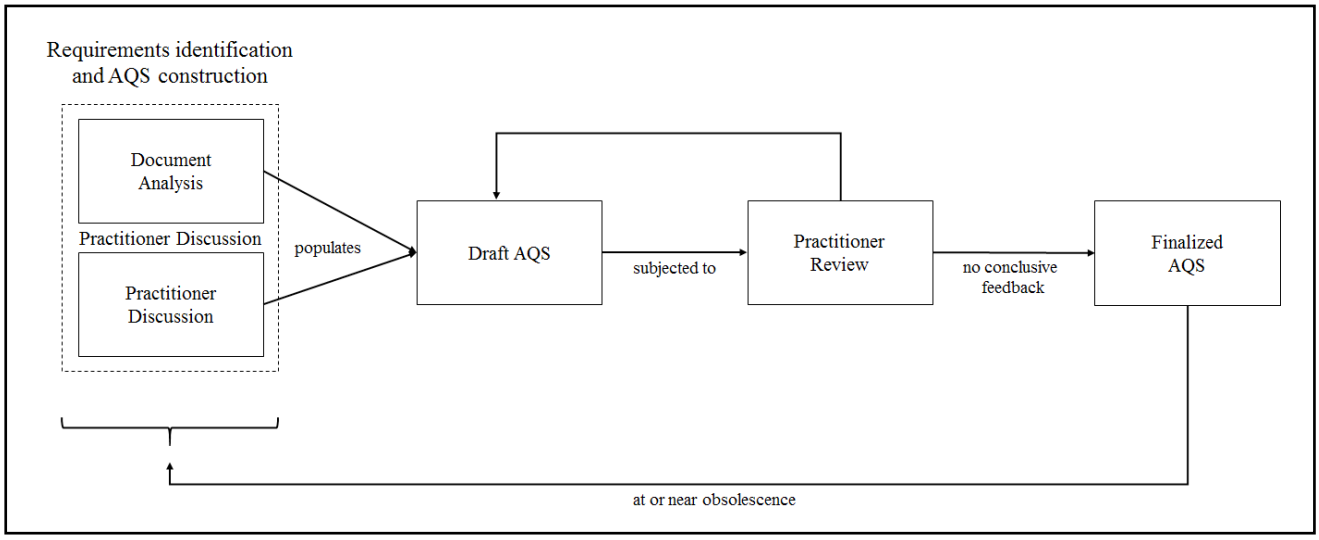


Figure 3. AQS finalization model - *Source: Author*

coding, to conduct pattern analyses. This will identify necessary job functions, classified as performance requirements, which populate the Applications Level of the AQS.

Further analysis of the identified Fundamentals and Applications Level requirements is used to generate the Systems Level requirements. By treating each of these requirements lists as documents, document analysis is applied to decompose the Applications Level requirements into the individual tools, techniques, or methods required, resulting in a list of simple systems for the Systems Levels. Document analysis is then applied to the Fundamentals Levels requirements; both validate the Applications Level requirements decomposition by mapping fundamental knowledge to required tools, techniques, and methods, to create a comprehensive list of simple systems required for qualification. Gaps that emerge from the validation, such as fundamental knowledge that is not represented in a simple system, are used to compose additional requirement as a collation(s) of this fundamental knowledge.

Section and Line Item Creation. After requirements identification is complete, the content from the AQS manifests as the creation of specific sections, within the Fundamentals, Systems, and Applications Levels, to classify and contain requirements. Individual line items are then generated to represent each requirement for these Levels. The process is conducted independently for each level in the AQS. Figure 2 presents this process.

> Using primitive coding on the requirements, the frequency and commonality of codes is used to group requirements into themes

The requirements list for each Level is treated as a narrative, and thematic analysis[1] is used to develop the sections in each Level. Using primitive coding[2] on the requirements, the frequency and commonality of codes is used to group requirements into themes. The resultant themes are identified, named, and converted into sections within the respective Level. Line items are created from the requirements in each section, using the originating data from inputs as a guide, to identify the knowledge or tasks that must be performed to satisfy the identified requirements. The result of application of this process is a qualification standard in which the Fundamentals, Systems, and Applications Levels all consist of individual sections, with lines items populated in each section. The Final Qualification Standard is not considered to be a separate Level, but rather the final section in the Applications Levels, consisting of the signatures of all board members

1 Thematic Analysis/coding is a form of qualitative analysis which involves recording or identifying passages of text or images that are linked by a common theme or idea.

2 Primitive data type is either of the following: a basic type is a data type provided by a programming language as a basic building block.

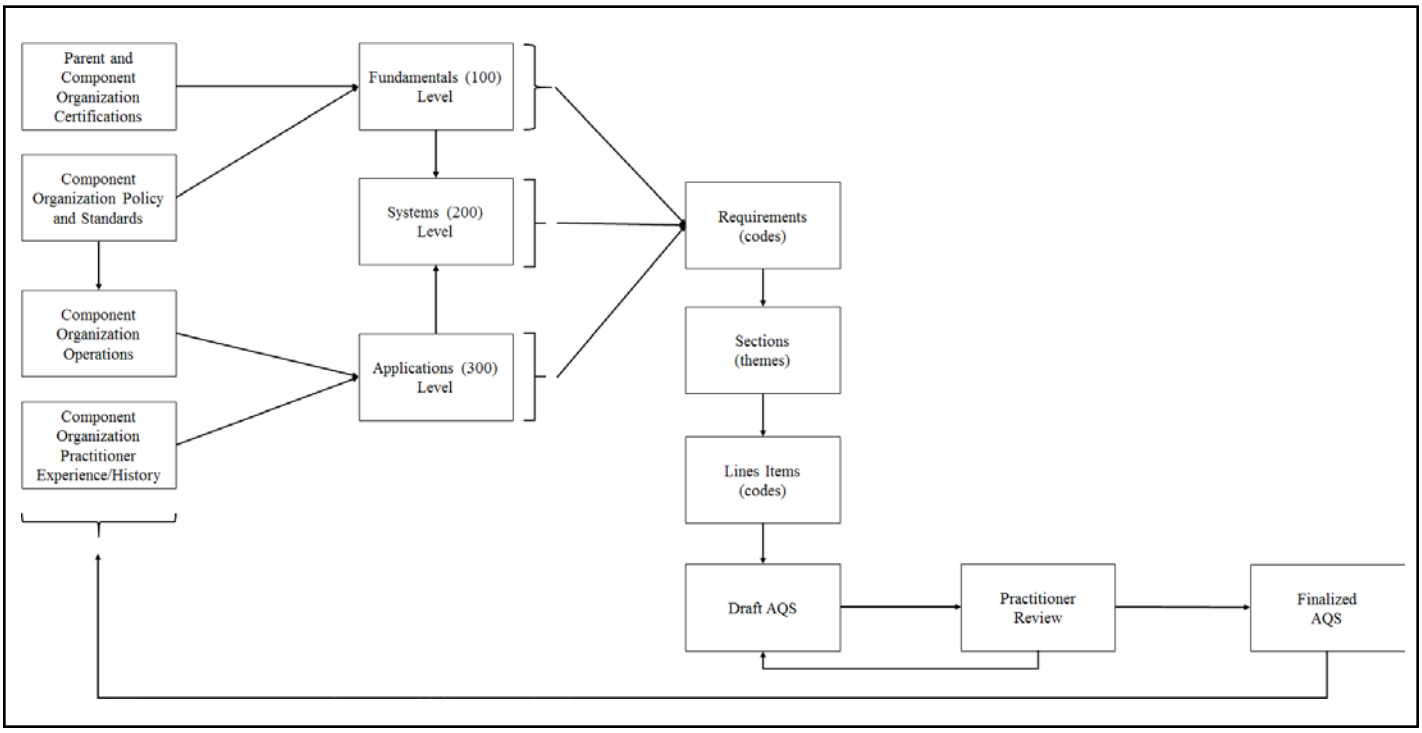


Figure 4. AQS Development Framework - *Source: Author*

indicating satisfactory completion of the required oral examination board. Conduct of this oral examination board is at the discretion of the component organization.

Standard Finalization. Finalization of the AQS is the final step prior to component organization deployment and is necessary to ensure the resultant AQS document satisfies the needs and requirements of the organization. Figure 3 illustrates the validation and fielding process for an AQS.

After document analysis and practitioners' inputs have been consolidated into a draft AQS, member checking is necessary to ensure validity and viability of the identified AQS. The member checking involves providing original practitioner participants with the draft AQS, soliciting all practitioner input, and consolidating feedback into revisions based upon requirements and dependencies present in the AQS. This process repeats iteratively and indefinitely until either no conclusive feedback is received or the component organization exhausts their available review time. At this time, the AQS draft is considered finalized AQS, and the qualification standard is distributed immediately and rapidly throughout the component organization using existing or established channels. At a minimum, the AQS and the instructions (including component organization requirements) for use and completion of the AQS should be distributed. Distribution of the first AQS will require these documents to be generated from scratch, but future AQS releases can repurpose existing documentation with minor revisions or changes. When the AQS is considered to be at or near obsolescence, the entire qualification standard is restarted.

Rapid Development and Deployment

Rapid development and subsequent deployment of the finalized AQS is necessary to preserve the relevance of the qualification standards. This strategic initiatives represent a manifestation of long-term planning which addresses organizational objectives and goals that may encompass the parent organization's mission requirements to include component's mission requirements; however, inherently it is not intended to address specific component's operational requirements. This, coupled with the continuous evolution of information technology and cybersecurity knowledge, creates volatile operational requirements; it also mandates rapid development and deployment of qualifications standards to ensure relevance for the longest possible period. Additionally, this manifestation must adapt with industry and operational changes to address qualification of component's operational requirements.

continuous evolution of information technology and cybersecurity knowledge, creates volatile operational requirements

Framework Presentation

The resultant framework for the development methodology is illustrated in Figure 4.

This framework represents the combination of the three models into a single method for rapidly developing an AQS to satisfy component organization requirements. First, using the requirements identification model, component organizations enumerate performance requirements using a combination of document analysis and personnel interviews, ultimately developing a requirements document for each of the three AQS Levels. The resultant requirements documents are inputs to the AQS construction model, in which primitive coding and thematic analysis are applied to item themes for sections and these Levels, and then decomposition is used to generate specific line items. This results in a fully populated draft AQS that is used as an input for the AQS finalization model, in which an iterative review and revision process is used to develop a finalized AQS for rapid deployment.

Discussion and Limitations

The AQS Development Framework represents a methodology that component organizations can use to rapidly develop their own qualification standards to augment and support the existing qualification requirements of their parent organizations. Using the framework and recommended methodology, organizations can reasonably expect to deploy AQS products rapidly enough to establish currency and relevancy and meet rapidly evolving operational requirements. When developing an AQS product, it is imperative for component organizations to minimize the amount of overlap with existing qualification standards. While some level of overlap is to be expected, particularly in the Fundamentals Level, substantial overlap represents a suboptimal situation, as the AQS is not augmenting existing standards but instead duplicating them. To this end, component organizations should strive to develop AQS products that are differentiated from their parent organization qualification standard with predominantly organization-specific knowledge and applications items.

There are inherent limitations in the use of the AQS Development Framework. The framework addressed the rapid development of an AQS product but assumes that a component organization has the means to rapidly distribute this product. In instances where this is not the case, component organizations will need to develop rapid distribution channels for the greatest viability. Additionally, the framework does not address the development of the supporting documentation necessary for the successful use of an AQS product. It is necessary for component organizations to, at a minimum, develop and deploy instructions and guidance for use and completion of an AQS product. Further, the framework reduces the extensive experience and tacit knowledge of component organization individuals and operations into a simplified series of line items. While this is a viable method to capture qualification requirements, there are inherent experiences and tacit knowledge that cannot be expressed in such a manner, and will inevitably be excluded from capture with this method. Finally, developers of the AQS standard will need to have, or develop, the ability to execute the primitive coding, thematic analysis, and decomposition skills to populate the AQS content. This means there may be additional workload by component organizations to prepare their environment for AQS use.

framework reduces the extensive experience and tacit knowledge of component organization individuals and operations into a simplified series of line items

Future Work

One major burden of the development of AQS using the AQS Development Framework is the decomposition and collation process necessary to populate line items for the Levels of the AQS. One possible method to overcome this would be future research that attempts to create prior codes, ideally realized through taxonomy development, that would provide developers with specific themes of knowledge areas to consider when developing the requisite line items. Additionally, as the use of the AQS Development Framework requires developers to execute primitive coding, thematic analysis, and decompositions—skills not always readily available in component organizations—further research into developing a simplified methodology of this process for practitioner or developer use could simplify the AQS development process.

REFERENCES

[1] Grenert, J. (2014). Personnel Qualification Standards Program (OPNAVINST 3500.34G).

[2] Grimes, J. (2005). Information Assurance Workforce Improvement Program (DoD Manual 8570.01).

[3] Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense strategy for operating in cyberspace and the attribution problem. AFL Review, 68, 167.

[4] Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3), 76-79.

[5] United States Navy. (2014). Personnel Qualification Standard Unit Coordinators Guide (NAVEDTRA 43100-1J).

ABOUT THE AUTHOR

Dr. Christopher Seedyk earned his Doctorate of computer science from Colorado Technical University. He now works at the US Army Research Laboratory. His research interests include human-centric cybersecurity, user behavior-efficacy modelling, and cyber intelligence.

Cyber Security & Information Systems
Information Analysis Center

Need Specialized Technical Support with Easy Contract Terms?

Core Analysis Task (CAT) Program

A Pre-Awarded, Pre-Competed Contract Vehicle.

CSIAC provides Subject Matter Expert (SME) support on an as-needed basis to quickly address technical requirements with minimal contracting effort. CSIAC provides such solutions via the utilization of our Core Analysis Task (CAT) service/capability. CSIAC is a competitively awarded contract with Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements. Custom solutions are delivered by executing user-defined and funded CAT projects without the need for further competition.

Through the CAT program, CSIAC is a pre-competed contracting vehicle, enabling the DoD and other agencies to obtain technical support for specific projects/programs that fall within one of the CSIAC technology areas. As with any inquiry, the first four hours are free. If the scope requires a CAT, CSIAC will assist with the development of a Performance of Work Statement (PWS) to be approved by the Contracting Officer's Representative (COR).

Key Advantages of working with CSIAC:

Expansive Technical Domain
The CSIAC's broad technical scope provides numerous pre-qualified resources for potential projects, and is especially valuable for today's information system challenges that frequently cross multiple domains.

Comprehensive STI Repositories
As a consolidation of three predecessor Information Analysis Centers (IACs), CSIAC has a wealth of expertise, data and information to support the successful completion of CATs.

Expansive Subject Matter Expert Network
CSIAC is able to leverage reach-back support from its expansive SME Network, including technical experts from the CSIAC staff, team members, or the greater community, to complete CATs.

Minimal Start-Work Delay
Not only does CSIAC provide DoD and other government agencies with a contract vehicle, but as a pre-competed single award CPFF IDIQ, work can begin in just a matter of weeks.

Apply the Latest Research Findings
CSIAC draws from the most recent studies performed by agencies across the DoD, leveraging the STI holdings of the Defense Technical Information Center (DTIC). The results of all CSIAC CATs and other DoD-funded efforts are collected and stored in DTIC's STI repository to support future efforts by the CSIAC and others.

How To Get Started

If you have a need for CSIAC technical support, the first step is to contact us. All Technical Inquiries are free to the customer for up to four hours of service. If the scope of the support is more extensive and requires a CAT, CSIAC will assist with the development and submission of the task description and related contract documents. CATs may be awarded as either Cost Plus Fixed Fee (CPFF) or Firm Fixed Price (FFP) delivery orders.

Inquiries may be submitted by email to **info@csiac.org**,
or by phone at **1-800-214-7921**.

Please visit our website for more information:
https://www.csiac.org/services/core-analysis-task-cat-program/

Who We Are

The Cyber Security Information Systems Information Analysis Center (CSIAC) is the DoD's Center of Excellence in Cyber Security and Information Systems, covering the following technical domains:

- Cybersecurity
- Software Engineering
- Modeling and Simulation
- Knowledge Management/ Information Sharing

CSIAC is chartered to leverage best practices and expertise from government, industry, and academia to solve the most challenging scientific and technical problems. The Center specializes in the collection, analysis, synthesis, and dissemination of Scientific and Technical Information (STI) to produce solutions in support of the defense community.

Our Team

Quanterion Solutions Incorporated is the prime contractor responsible for operating the CSIAC. In addition to Quanterion, customers also have access to the other members of the CSIAC team which include leading technology corporations as well as prestigious academic institutions that perform cutting edge research activities to expand our knowledge base.

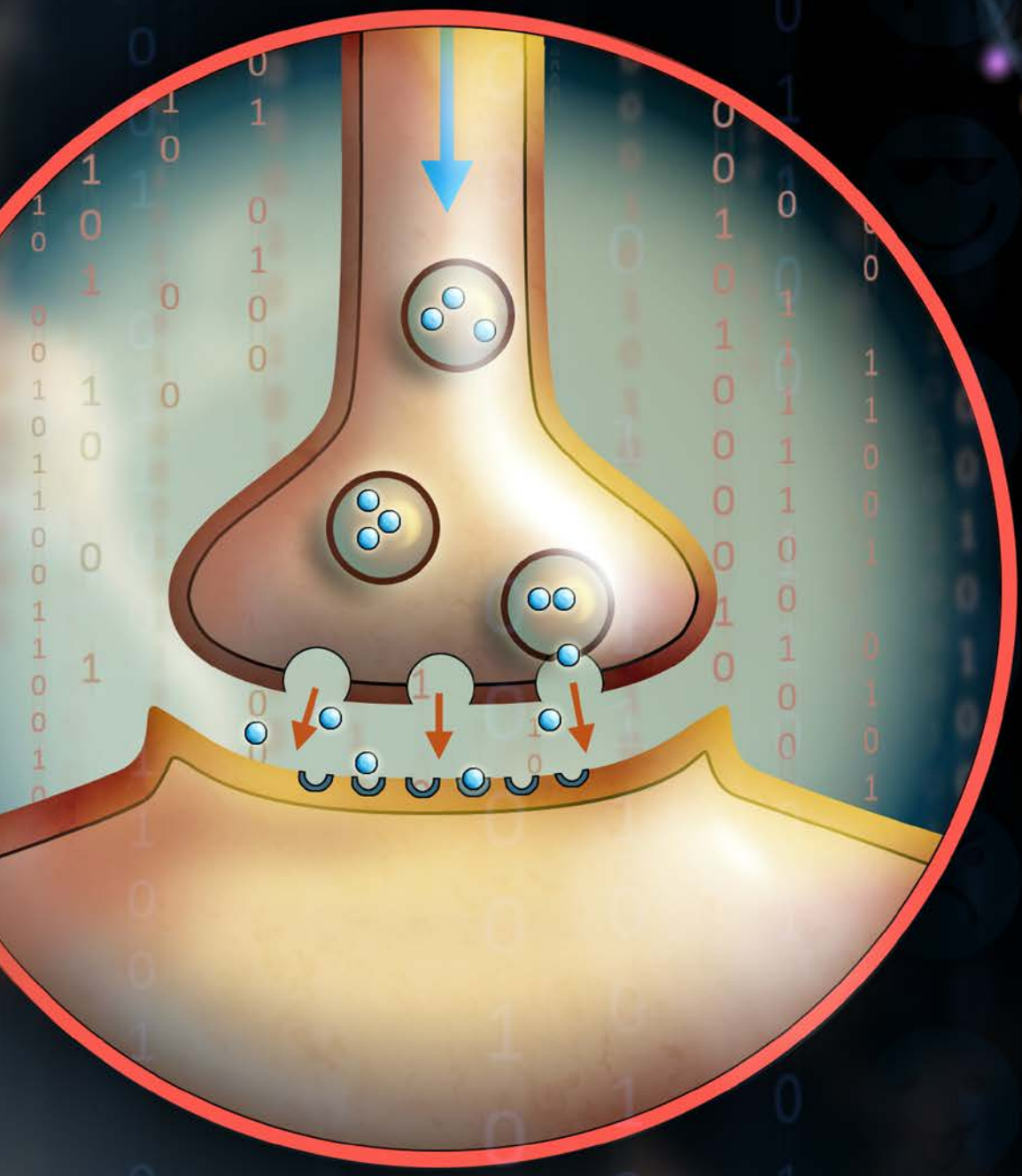
Cyber Security & Information Systems
Information Analysis Center

266 Genesee Street
Utica, NY 13502

1-800-214-7921
https://www.csiac.org

ENDURING, FLEETING, FUTURE:

A brief overview of current sentiment and emotional analysis, a look forward



By Dr. Erik Wemlinger

Sentiment and emotion analysis are two critical technologies that will assist as we continue to transition from the industrial age into the information age.

Sentiment analysis is critical in the development of automated data curation, and knowledge management, and cybersecurity. Both sentiment and emotion analysis are needed to improve the human-machine interface and to support human-machine interactions and teaming in complex environments.

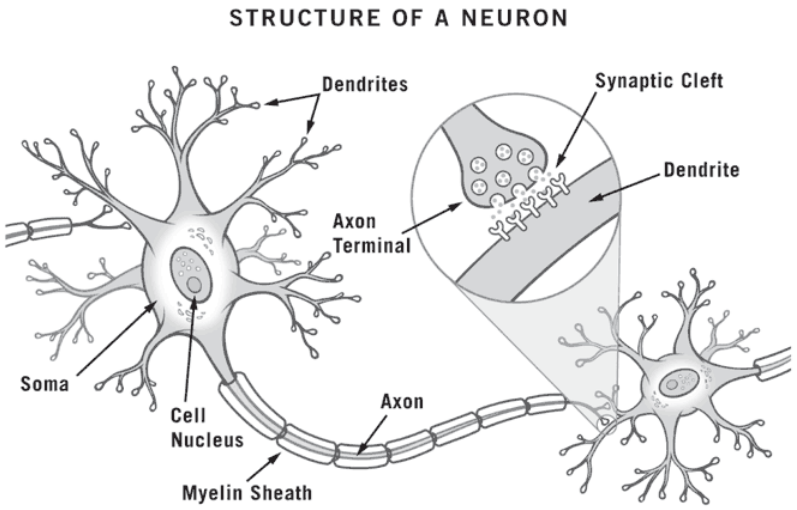


Figure 1. Basic structure of a neuron [21] - *Source: Author*

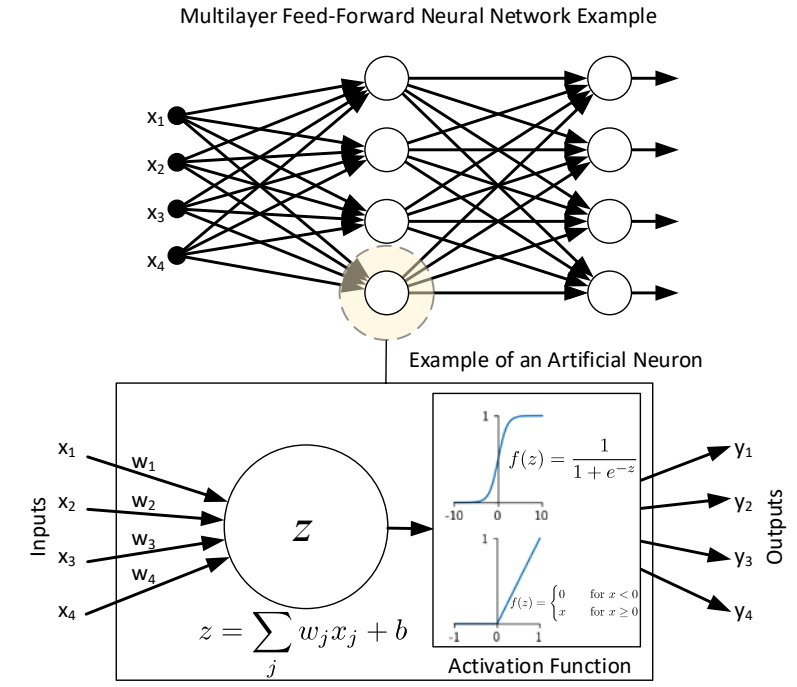


Figure 2. Example of a multilayer FNN [19] - *Source: Author*

Introduction

Sentiment and emotion analysis are critical tools in knowledge aggregation and interfacing with people. As we move from the industrial age, where wealth is measured in capital, into the information age, Barbara Endicott-Popovsky suggests that knowledge will be the new measure of wealth [1]. According to Addleson, knowledge management typically takes two approaches, either focus on people as knowledge workers or on the tools and data [2]. With the rapid development of neural networks, these two knowledge management foci can merge as machines become the knowledge workers. As machines take on the role of knowledge workers, there will be an increased need for machines to recognize emotion as well as sentiment. Current state of the art methods for machines to distinguish sentiment and emotions utilize artificial neural networks.

This article will discuss artificial neural networks and how they are used in emotion and sentiment analysis, as well as a look into how these technologies can allow machines to be a more integral part of knowledge management and the cyber domain.

In this article, the use of sentiment analysis is based on Scherer's typology of affective states [3, 4, 5]. According to Scherer, sentiment analysis focuses on attitudes, which are enduring beliefs towards objects or persons. Due to the enduring nature of sentiment, written views are a common source for this analysis. Following Scherer's typology, emotion is considered a brief organically synchronized event; thus, emotion analysis is highly temporal and triggered by any and all stimuli. In terms of emotional analysis and detection, the focus will be on the seven universal emotions identified by Ekman [6]; joy, surprise, fear, anger, sadness, disgust, and contempt [6]. The data used as the basis for emotional analysis, as discussed in this article, focuses on images or video capturing a specific emotion in time. Analysis of these two affective states requires different approaches due to the medium by which they are conveyed.

Background

Modern sentiment and emotion analysis are built on decades of psychological research. Natural Language Processing (NLP) is critical for sentiment analysis based on the use of statistics as discussed by Manning and Schütze [7]. With an understanding of word usage frequency, various methods can be used to assign a sentiment by sentence, paragraph, or even larger portions of text. Supervised and unsupervised sentiment analysis are the two approaches used. These methods typically utilize a sentiment lexicon coupled with some machine learning algorithm like the following exemplars: bagging, K-Means, support vector machine or naive Bayes classifiers and/or some form of a hybrid [8, 9, 10, 11].

Just as NLP is a critical stepping stone for work in sentiment analysis, computer vision is critical to the area of automated emotion detection [12, 13]. Ekman [14] devised the Facial Action Coding System (FACS), which

mapped facial muscles known as, or Action Units (AU), and combinations of AU to the facial expressions related to the seven universal emotions. Various methods have been used to automate emotion detection from video and images, as well as other factors, like attention. Initially, basic facial landmark methods were used to establish an AU, and from there, a probability of the associated emotion was calculated [12, 15]. While the trend for emotion detection is moving towards artificial neural networks, the field is still young. There has been considerable exploration of the other methods for emotion detection from images and video. These other methods typically leverage computer vision techniques like Histogram of Oriented Gradients (HOG), Histogram of Image Gradient Orientation (HIGO), Histograms of Optical Flow (HOF), Local Binary Patterns (LBP) coupled with Support Vector Machines (SVM) or support vector regression (SVR) [16, 17].

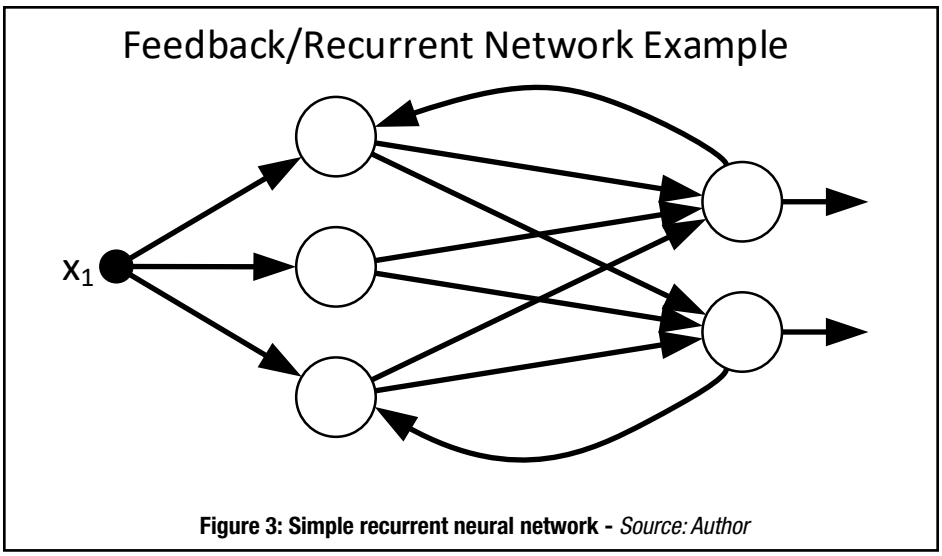


Figure 3: Simple recurrent neural network - *Source: Author*

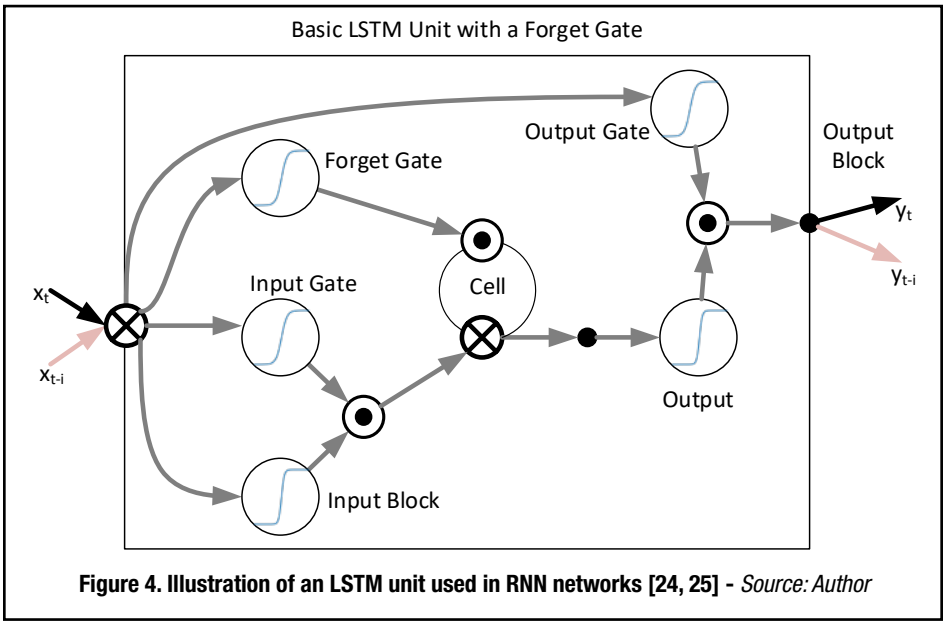


Figure 4. Illustration of an LSTM unit used in RNN networks [24, 25] - *Source: Author*

Current Technologies

Artificial Neural Networks

The computational model for an artificial neural network was proposed in 1943 by McCulloch and Pitts [18], when trying to understand how cats and monkeys process information from the eyes. Computational limitations greatly hampered widespread use and simpler machine learning methods such as SVMs. The increase of computational power and the need for more sophisticated machine learning solutions that are less sensitive to noise has resulted in a resurgence of interest in artificial neural networks.

The promise of Artificial Neural Networks (ANN) is to move beyond the von Neumann computer architecture [19]. The von Neumann approach has resulted in computers that can outperform people in the numeric domain. However, there is a need for algorithms that can learn and adapt in order to solve new problems such as sentiment analysis and emotion detection.

Understanding ANNs starts with understanding the neural networks on which the ANNs are modeled. Typical neurons have three components: inputs (dendrites), the cell body (soma), and the output (axon) [20]. Each neuron has multiple inputs which go into the soma. From there, a neural network is formed by a single axon branching out from the soma, connecting to other neural networks via their dendrites. Figure 1 illustrates the structure of a neuron showing the inputs via the dendrites on the left, where the signals travel through the soma and then, depending on the inputs, a signal may be sent out via the axon.

The axon will branch in order to connect to multiple other neurons. The connection from the axon to the dendrite of another neuron is called a synapse. The speed (much slower than electrical signals) that the signals travel in a neural network, when compared to time it takes for a response to stimuli, suggests that signal processing takes less than 100 stages [19].

Figure 2 illustrates a Feed-Forward Neural network (FNN), the first of two major types of ANNs, with multiple layers. The bottom neuron or node is highlighted to illustrate how the node processes a signal input [19]. For each node, the inputs are multiplied by learned weights (wj) and summed. Weights can be positive or negative, consistent with exciting a neuron or inhibiting a neuron. To this sum, a learned bias value is added (b). This sum is given to an activation function, of which there are many. Two of the most popular are the sigmoidal curve and the Rectified Linear Unit (ReLU). Some of the first neural networks utilized a unit step function acting as a binary neuron. For the majority of applications, the sigmoid or ReLU have replaced the unit step because they are

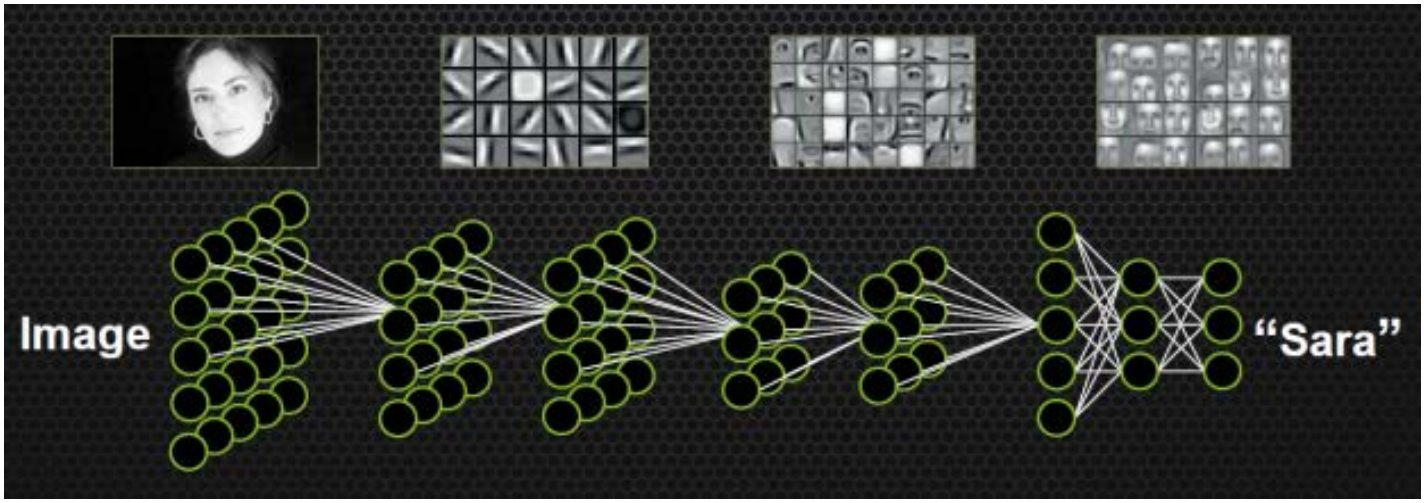


Figure 5. Example of a convolutional neural network (CNN) for facial recognition [29, 48] - *Source: Author*

differentiable, making learning methods like gradient descent easier. The nodes in the next layer that are connected to this highlighted node receive the output of the activation function and begin the process over again.

The feed-forward ANN, once trained, can be deployed and will not adapt or continue learning. The second major type of ANN is the Recurrent or Feedback Neural Network (R/FNN). This is illustrated in Figure 3 which shows a basic ANN with feedback. These types of networks continue to learn to adapt to changes, the complication being that training is slow and can stop if the gradient goes to zero [22]. To address this, a long short-term memory unit (LSTM) was proposed. LSTM maintains a constant error along with the ability to forget and reset its state [23, 24, 25]. A long short-term memory LSTM units can continue to learn over 1,000 time steps. Figure 4 is an illustration of an LSTM unit. This unit uses weighted inputs summed with past inputs, which are then sent to an input activation function and activation functions that make up the input, output, and forget gates. The activation functions are typically sigmoid or tanh. The center contains the cell, which stores a continuous error of one multiplied by the output of the forget gate. The result of this multiplication is summed with the product of the input and input gate. The sum from the forget and input products goes to an output activation function, which is multiplied by the output gate.

While the LSTM unit is more complicated than the simple neuron/node seen in Figure 2, it outperforms a traditional RNN. The benefit of the RNN type network (including the LSTM) is its ability to process temporal data or sequences, which is why these types of networks are typically used for sentiment analysis.

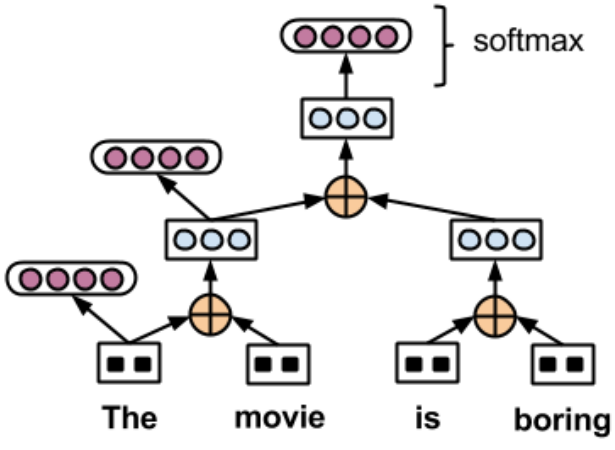


Figure 6. This figure illustrates how an LSTM-RNN network can be constructed for sentiment analysis [34]. The yellow filled cross-hairs are the LSTM units, the softmax layer calculates the sentiment probability - *Source: Author*

CNNs and Emotion Detection

Convolutional neural networks (CNN), a type of FNN, were inspired by looking at the visual cortex of cats and monkeys, which contain locally-sensitive, orientation-selective neurons [26, 27, 28]. This type of structure has proven to work well for visual analysis. CNNs are trained feature filters, which work well at identifying features that are related spatially. Figure 5 illustrates this starting with an image on the left and moving to the right; this represents showing the first set of filters in the convolutional neural network [29]. The first filter is shown as the image directly to the right of the original image in Figure 5, highlighting the very basic edge/line detection. From there, additional filters are applied, each one adding a convolutional layer, which is more abstract than the previous (shapes, contours, objects). By the last layer, parts of a face can be identified, such as eyes, mouth and so on. The last layer in this CNN example are portions of the faces used to train the filters. Neural networks require large quantities of training data to ensure that generic features are identified and that overfitting does not occur.

Modern emotion detection methods utilize CNN for their utility in image identification [30, 31, 32, 33]. The CNN is used to classify an observed emotion on static images and relating them to the previously mentioned Action Units. As mentioned before, neural

networks require large amounts of data and considerable computational power for training. However, once trained, a neural network classification is very efficient and typically exhibits higher accuracy when compared to other existing machine learning methods.

RNNs and Sentiment Analysis

While CNNs work well when information is related spatially, RNNs work well when looking at temporal or sequential information. RNNs have input, output, and hidden nodes which are connected to create an internal memory. This allows for the processing of arbitrary sequences, but these types of networks are very susceptible to vanishing or exploding feedback. If the feedback vanishes, no learning occurs. On the other hand, if the feedback explodes, incorrect learning can occur. LSTM units, a type of RNN themselves, are typically used in modern RNN, resulting in a stable learning network [23, 34]. The LSTM has been described as a low pass filter, keeping high frequency noise from confusing the answer [35]. Figure 6 illustrates an LSTM-RNN network used for sentiment analysis [34]. The LSTM units are the yellow filled cross-hairs. In a standard RNN network, these units would simply be removed and each word would go into the blue RNN layer. The outermost layer, known as the softmax layer, is used to calculate the sentiment probability of neutral, positive, or negative, along with the classification of the sentence as a whole.

Looking Ahead

RNNs and CNNs are currently the most common neural networks, but there are others and researchers are continuing to build deeper networks. Combining the benefits of a learned network found in CNNs with the ability to adapt and learn over time, has resulted in ANN, which are combinations of both architectures [36, 37, 38]. This is typically done by starting with a trained CNN and connecting that to a RNN, providing both spatial and temporal reasoning.

Generative Adversarial Networks (GANs)[1], which combine multiple NNs in a very different way to provide surprisingly effective optimizations, are showing benefit in several areas.

In terms of human-AI teaming and applications to the cyber domain, there is even work moving ahead on helping humans understand the AI's "point of view" to better solve problems and meet complex goals.[2]

Conclusion

With the development of more advanced ANNs and the integration of as machines become integrated into the process, knowledge management will become diverse with people, tools, and data. Improving human-machine interactions through emotional intelligence is crucial in developing trust between people and machines [39]. Advances to neural network algorithms, and better-quality computational capability are enabling better emotion and sentiment detection systems. This results in improving the human-machine interface as well as the machines ability to manage knowledge and interpret human interactions more effectively.

Companies from a variety of industries have been developing their own emotion detection systems or buying up other companies with experience in emotion detection [40, 41, 42, 43]. Most, if not all of these companies, are utilizing neural networks to understand emotions, and developing automated sentiment analysis for text, as well as voice analysis, to improve human-machine interactions [44]. In the cyber domain, there is much work going on in the area of combined human-machine teams that require emotion and sentiment understanding to stand up to the sometimes complex scenarios of cybersecurity.

Neural networks are still in their infancy and it will be a moment while before neural networks will be able to think like a human due to the limited complexity of the neural networks currently possible. Williams and Herrup [45] have looked at the total number of neurons in different species central nervous systems. They found that small organisms, like metazoans, typically had less than 300 neurons, while the common octopus and small mammals, like mice, have between 30 – 100 million neurons. Larger mammals, like whales and elephants, have more than 200 billion neurons. Healthy adult humans of normal intelligence have an estimated 100 billion neurons. Estimates for the current number of neural units used in ANN is in the millions for the most complex networks [46]. However, with the continued increase in computing power and introduction of new computational designs like neuromorphic commuting, closing the gap is just a matter of time [47, 21].

outermost layer, known as the softmax layer, is used to calculate the sentiment probability of neutral, positive, or negative

1 This also should be a citation, I don't want to try to do that... reference is "Generative Adversarial Nets" by Ian Goodfellow, arXiv:1406.2661v1 [stat.ML] 10 June 2014

2 This could be a citation as well (probably should be for coherence with the rest of the article) – reference is "It Takes Two to Tango: Towards Theory of AI's Mind" , Chandrasekaran, arXiv:1704.00717v2 [cs.CV] 2 Oct 2017

REFERENCES

[1] B. Endicott-Popovsky, "The Probability of 1," *Journal of Cyber Security and Information Systems*, vol. 3, pp. 18-19, 2015.

[2] M. Addleson, "A Knowledge Management (KM) Primer," *Journal of Cyber Security and Information Systems*, vol. 2, pp. 2-12, 2014.

[3] K. R. Scherer, "Emotion as a multicomponent process: A model and some cross-cultural data.," *Review of Personality & Social Psychology*, 1984.

[4] C. Potts, "Sentiment Symposium Tutorial," 2011 (accessed December 7, 2016).

[5] K. R. Scherer, "What are emotions? And how can they be measured?," *Social science information*, vol. 44, pp. 695-729, 2005.

[6] P. Ekman, Telling lies: Clues to deceit in the marketplace, politics, and marriage (revised edition), WW Norton & Company, 2009.

[7] C. D. Manning and H. Schütze, Foundations of statistical natural language processing, vol. 999, MIT Press, 1999.

[8] X. Hu, J. Tang, H. Gao and H. Liu, "Unsupervised sentiment analysis with emotional signals," in *Proceedings of the 22nd international conference on World Wide Web*, 2013.

[9] B. Pang, L. Lee and S. Vaithyanathan, "Thumbs up?: sentiment classification using machine

learning techniques," in *Proceedings of the ACL-02 conference on Empirical methods in natural language processing-Volume 10*, 2002.

[10] B. Pang and L. Lee, "A sentimental education: Sentiment analysis using subjectivity summarization based on minimum cuts," in *Proceedings of the 42nd annual meeting on Association for Computational Linguistics*, 2004.

[11] T. Mullen and R. Malouf, "A Preliminary Investigation into Sentiment Analysis of Informal Political Discourse.," in *AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs*, 2006.

[12] Z. Zeng, M. Pantic, G. I. Roisman and T. S. Huang, "A survey of affect recognition methods: Audio, visual, and spontaneous expressions," *IEEE transactions on pattern analysis and machine intelligence*, vol. 31, pp. 39-58, 2009.

[13] R. Hartley and A. Zisserman, Multiple view geometry in computer vision, Cambridge university press, 2003.

[14] P. Ekman, W. V. Friesen and J. C. Hager, "Facial action coding system (FACS)," *A technique for the measurement of facial action. Consulting, Palo Alto*, vol. 22, 1978.

[15] G. Littlewort, J. Whitehill, T. Wu, I. Fasel, M. Frank, J. Movellan and M. Bartlett, "The computer expression recognition toolbox (CERT)," in *Automatic Face & Gesture Recognition and Workshops (FG 2011)*, 2011 IEEE International Conference on, 2011.

[16] Y. Song, L.-P. Morency and R. Davis, "Learning a sparse codebook of facial and body microexpressions for emotion recognition," in *Proceedings of the 15th ACM on International conference on multimodal interaction*, 2013.

[17] X. Li, X. Hong, A. Moilanen, X. Huang, T. Pfister, G. Zhao and M. Pietikäinen, "Reading hidden emotions: spontaneous micro-expression spotting and recognition," *arXiv preprint arXiv:1511.00423*, 2015.

[18] W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The bulletin of mathematical biophysics*, vol. 5, pp. 115-133, 1943.

[19] A. K. Jain, J. Mao and K. M. Mohiuddin, "Artificial neural networks: A tutorial," *Computer*, vol. 29, pp. 31-44, 1996.

[20] N. Baumann and D. Pham-Dinh, "Biology of oligodendrocyte and myelin in the mammalian central nervous system," *Physiological reviews*, vol. 81, pp. 871-927, 2001.

[21] T. Pfeil, "Exploring the potential of brain-inspired computing," 2015.

[22] Z. C. Lipton, J. Berkowitz and C. Elkan, "A critical review of recurrent neural networks for sequence learning," *arXiv preprint arXiv:1506.00019*, 2015.

[23] F. A. Gers and E. Schmidhuber, "LSTM recurrent networks learn simple context-free and context-sensitive languages," *IEEE Transactions on Neural Networks*, vol. 12, pp. 1333-1340, 2001.

[24] F. A. Gers, J. Schmidhuber and F. Cummins, "Learning to forget: Continual prediction with LSTM," *Neural computation*, vol. 12, pp. 2451-2471, 2000.

[25] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink and J. Schmidhuber, "LSTM: A search space odyssey," *IEEE transactions on neural networks and learning systems*, 2016.

[26] Y. LeCun and Y. Bengio, "Convolutional networks for images, speech, and time series," *The handbook of brain theory and neural networks*, vol. 3361, p. 1995, 1995.

[27] M. Matsugu, K. Mori, Y. Mitari and Y. Kaneda, "Subject independent facial expression recognition with robust face detection using a convolutional neural network," *Neural Networks*, vol. 16, pp. 555-559, 2003.

[28] D. H. Hubel and T. N. Wiesel, "Receptive fields and functional architecture of monkey striate cortex," *The Journal of physiology*, vol. 195, pp. 215-243, 1968.

[29] H. Lee, R. Grosse, R. Ranganath and A. Y. Ng, "Convolutional deep belief networks for scalable unsupervised learning of hierarchical representations," in *Proceedings of the 26th annual international conference on machine learning*, 2009.

[30] S. Albanie and A. Vedaldi, "Learning Grimaces by Watching TV," *arXiv preprint arXiv:1610.02255*, 2016.

[31] P. O. Glauner, "Deep convolutional neural networks for smile recognition," *arXiv preprint arXiv:1508.06535*, 2015.

[32] S. Zafeiriou, A. Papaioannou, I. Kotsia, M. Nicolaou and G. Zhao, "Facial Affect "in-the-wild": A survey and a new database," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2016.

[33] S. Zweig and L. Wolf, "InterpoNet, A brain inspired neural network for optical flow dense interpolation," *arXiv preprint arXiv:1611.09803*, 2016.

[34] P. Le and W. Zuidema, "Compositional distributional semantics with long short term memory," *arXiv preprint arXiv:1503.02510*, 2015.

[35] Y. Bengio, N. Boulanger-Lewandowski and R. Pascanu, "Advances in optimizing recurrent networks," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013.

[36] P. Khorrami, T. Le Paine, K. Brady, C. Dagli and T. S. Huang, "How deep neural networks can improve emotion recognition on video data," in Image Processing (ICIP), *2016 IEEE International Conference*, 2016.

[37] L. Deng and J. Platt, "Ensemble deep learning for speech recognition," 2014.

[38] T. N. Sainath, O. Vinyals, A. Senior and H. Sak, "Convolutional, long short-term memory, fully connected deep neural networks," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference*, 2015.

[39] T. Heffernan, G. OŃeill, T. Travaglione and M. Droulers, "Relationship marketing: The impact of emotional intelligence and trust on bank performance," *International Journal of bank marketing*, vol. 26, pp. 183-199, 2008.

[40] *Google Cloud Vision API*.

[41] IANS, *Facebook acquires emotion detection startup FacioMetrics*, 2016 (accessed January 17, 2017).

[42] *Microsoft Cognitive Services Emotion API*.

[43] C. Metz, "Apple Buys AI Startup That Reads Emotions in Faces," 2016 (accessed January 17, 2017).

[44] B. Doerrfeld, *20+ Emotion Recognition APIs That Will Leave You Impressed, and Concerned*, 2015 (accessed January 17, 2017).

[45] R. W. Williams and K. Herrup, "The control of neuron number," *Annual review of neuroscience*, vol. 11, pp. 423-453, 1988 (accessed February 27, 2017).

[46] Wikipedia, *Artificial neural network --- Wikipedia*, The Free Encyclopedia, 2017.

[47] D. S. Modha, "Introducing a Brain-inspired Computer," accessed January 19, 2017.

[48] L. Brown, "Accelerate Machine Learning with the cuDNN Deep Neural Network Library," NVIDIA Accelerated Computing, 7 9 2014. [Online]. Available: https://devblogs.nvidia.com/parallelforall/accelerate-machine-learning-cudnn-deep-neural-network-library/. [Accessed 7 3 2017].

ABOUT THE AUTHOR

Dr. Wemlinger is a Senior Data Scientist at Syracuse Research Corporation (SRC) with over 15 years of research experience in the areas of low-pressure high-temperature plasma, high-pressure low-temperature plasma, energetic materials, finite element modeling, physics education, data analysis, and algorithm development. He is skilled at integration of disparate technologies in the development of novel solutions, concept development and testing, iterative concept improvement, and team development. Dr. Wemlinger also serves as a Team Supervisor in the Intelligence Systems & Analytics efforts.

R&E Gateway

Powered by DTIC

https://www.dtic.mil

Propel your research, gain new insights and bring to life your warfighter technology concepts and solutions.

- *Over 4 Million Technical Reports*
- *DoD Research Projects*
- *DoD-Published R&E Journal*
- *Planned Research*
- *24x7 Virtual Workspace*

Get started at

https://go.usa.gov/xQAbm

The Defense Technical Information Center (DTIC) is DoD's authoritative source for scientific and technical (S&T) information. For more information on DTIC contact **1-800-225-DTIC (3842)**, and choose **option 1** or email: **dtic.belvoir.us.mbx.reference@mail.mil**

CYBER OPERATIONAL ARCHIT
TRAINING SYSTEM - CYBER FO

By: Dr. David "Fuzzy" Wells, IPA, CMSP and Derek Bryan

TECTURE OR ALL

Current methods for conducting cyber training are incompatible with the traditional, simulation-based training architectures used to conduct battlestaff training. As a result, there is little to no interaction between the cyber domain and the traditional warfighting domains during exercises.

This situation does not accurately reflect the current operational environment nor does it address the Secretary of Defense's (SECDEF) and the Chairman of the Joint Chiefs of Staff's (CJCS) directives and guidance for incorporating realistic cyberspace conditions into major Department of Defense (DoD) exercises.

The Cyber Operational Architecture Training System (COATS) is a U.S. Defense Modeling & Simulation Coordination Office (DMSCO) High-Level Task (HLT) that integrates existing cyber range environments, traditional simulation architectures, operational networks, and cyber emulations to safely and securely synchronize and deliver realistic cyber effects to the entire battlestaff – cyber for all. In doing so COATS provides an integrated and contested training environment where operators plan, execute and experience realistic cyberspace operations and conditions in all domains. This article describes the key components of the COATS architecture, including the application of network guards and the first draft of a cyber Data Exchange Model (DEM). This article also outlines lessons learned from the demonstration and employment of COATS during three U.S. Forces Korea exercises, U.S. Navy Fleet Synthetic Training (FST) events, and Operation Blended Warrior (OBW) at the annual Interservice/Industry Training, Simulation and Education Conference (I/ITSEC). Recommendations for future cyber and traditional modeling and simulation capability research, development, test and evaluation are also included.

Operational Problem

There is no controversy regarding the realities of cyber threats to U.S. interests at home and abroad. The DoD, in partnership with international, federal, state and local governments is tasked with defending those interests and enabling an open, secure and prosperous cyberspace environment for all. The April 2015 DoD Cyber Defense Strategy guides the development of cyber capabilities necessary to organize, train, and equip U.S. military forces in these missions. This guidance calls for the development of "… an individual and collective training capability … to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks" (Carter, 2015).

The majority of today's cyber training is conducted on dedicated, closed network "ranges" that provide the basic services and controls necessary to train DoD Cyber Mission Forces on their primary tasks and missions. While sufficient for this purpose, these ranges operate independently from the traditional M&S environments used to conduct battlestaff training across the spectrum of DoD operations, many of which are influenced by or rely on the cyber domain. As a result, there is a lack of integration with the cyber domain during major DoD exercises that limits the battlestaff's ability to plan, integrate, and execute integrated cyber operations. Perhaps more importantly, this limitation restricts the battlestaff's opportunities to experience and fight through degraded and denied conditions as required by the April 2014 CJCS Instruction 3500.01H entitled "Joint Training Policy for the Armed Forces of the United States" (Goldfein, 2014). Manual workarounds (e.g., "white cards") can be used by exercise controllers to inject rudimentary degraded or denied conditions into exercises, but these workarounds are typically low fidelity and have little or no relation to the ongoing cyber war within the cyber ranges or the M&S environment used to stimulate the Command, Control, Communications, Computers and Information (C4I) systems in use by the battlestaff. Furthermore, white cards do not allow the training audience the opportunity to realistically detect, assess, and respond to a cyber attack. This situation is summarized in Figure 1 below.

Coats Description

In 2014 DMSCO funded an HLT to develop an integrated training environment prototype capable of addressing the operational needs described above. COATS leverages and integrates existing cyber range environments, traditional battlestaff training architectures, operational networks, and cyber emulations to synchronize and deliver realistic cyber and traditional effects to the entire battlestaff. This integration is facilitated by the use of a network guard to protect and assure data flow between disparate networks and a new cyber Data Exchange Model (DEM) for interoperability between cyber and traditional M&S systems as depicted in Figure 2.

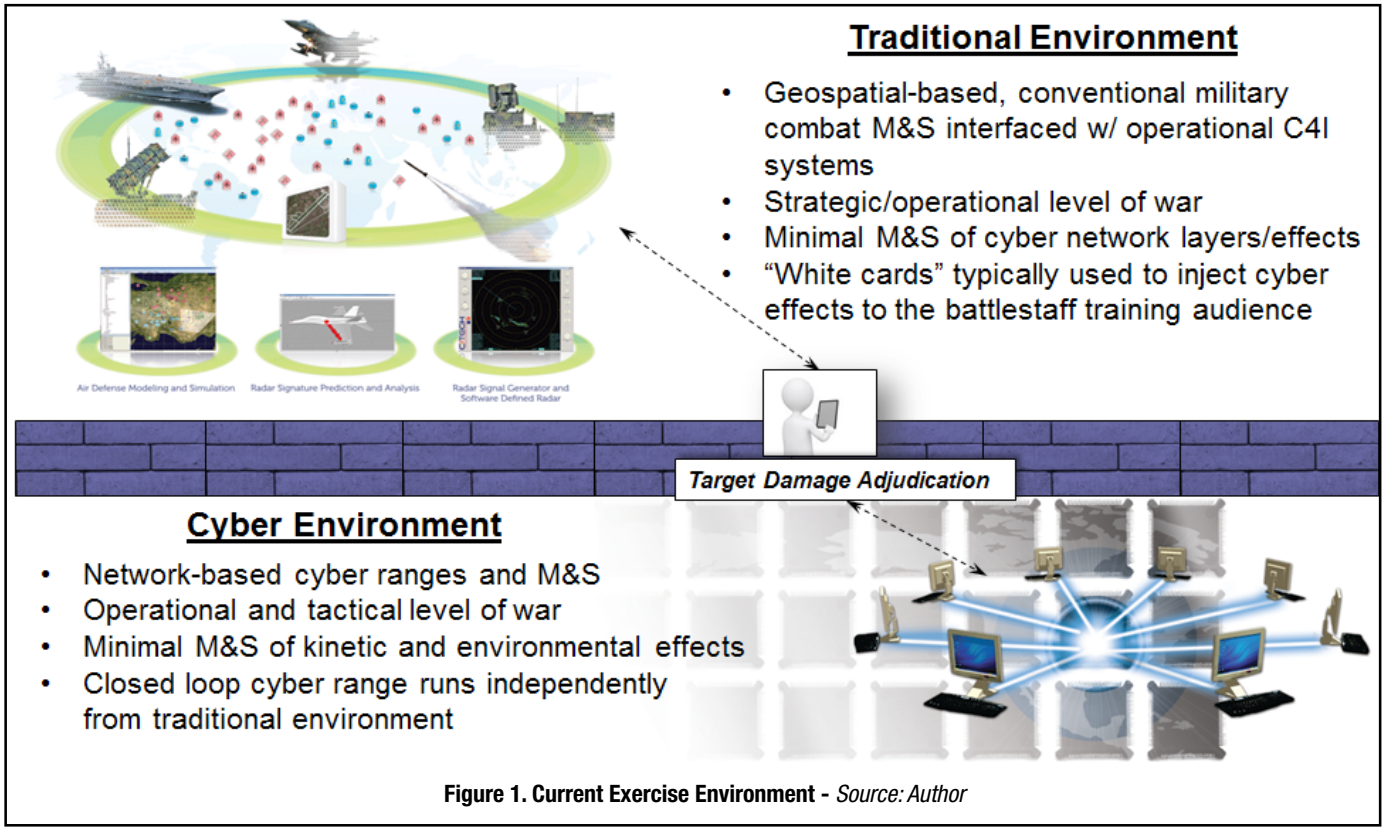


Figure 1. Current Exercise Environment - *Source: Author*

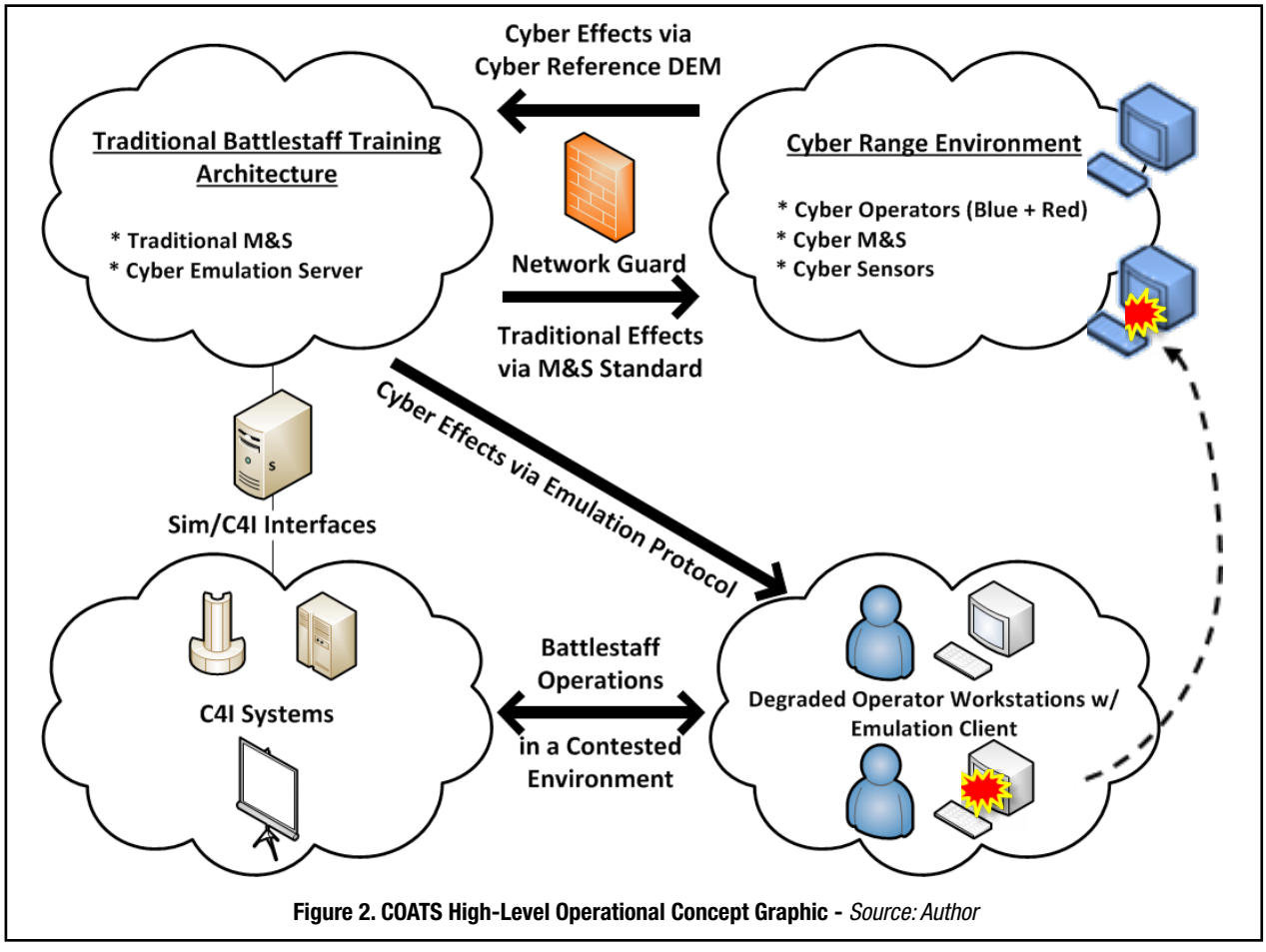


Figure 2. COATS High-Level Operational Concept Graphic - *Source: Author*

The critical components of the COATS architecture are the following:

- **Cyber Range Environment** – The cyber range environment is a collection of Live, Virtual and Constructive (LVC) cyber M&S tools and sensors used to create a realistic representation of critical networks, nodes, systems and message traffic correlated with the overall exercise scenario and forces. The cyber range environment is responsible for sensing cyber effects (not attacks) of interest, translating cyber effects into the cyber DEM, and passing over a protected network to the traditional battlestaff training architecture. Message traffic must pass through a network guard prior to receipt by the traditional battlestaff training architecture. A combination of open source, Government-Off-The-Shelf, Commercial-Off-The-Shelf and custom tools are used to create the cyber range environment such as Nagios, iperf, the Joint Network Simulation (JNETS) component of the USAF's Air and Space Constructive Environment Information Operations Suite (ACE-IOS), and EXata. The cyber range is also responsible for receiving traditional effects of interest (e.g., kinetic and Electronic Warfare [EW] effects) from the traditional battlestaff training architecture and simulating those effects on the corresponding cyber range networks, nodes, systems and message traffic. Example effects include performance degradation, configuration changes and system failure.
- **Cyber DEM** – The cyber DEM is a draft standard developed by COATS partners that organizes and defines a series of data types that represent cyber effects of interest. The cyber DEM is necessary because there is no existing standard or method for sharing cyber M&S data within the DoD. Currently implemented as an eXtensible Markup Language (XML) schema, the cyber DEM can be easily applied to a DoD M&S standard such as the Distributed Interactive Simulation, High-Level Architecture, or the Test and Training Enabling Architecture (Morse, Drake, Wells, Bryan, 2014). The cyber DEM has been implemented as an XML schema in the U.S. Army's Joint Land Component Constructive Training Capability (JLCCTC) federation and as a set of HLA objects and interactions in the U.S. Navy's Navy Training Federation Object Model. The U.S. Air Force and the National Guard are both evaluating the cyber DEM as an extension to the DIS Information Operations Protocol Data Unit (PDU).
- **Network Guard** – An accredited network guard is required between the cyber range environment and the traditional battlestaff training architecture to assure and protect the applicable networks and systems. The network guard implements a restrictive ruleset that ensures that only approved messages, in the proper format, are securely passed from the expected sender to the expected receiver and vice versa. The network guard does not change or validate the classification level of the data. The U.S. Navy's Radiant Mercury (RM) device, in tandem with the USAF's ACE-IOS "Joint. Information Operations Range (JIOR) Broker" application, collectively acts as the network guard for COATS.
- **Traditional Battlestaff Training Architecture** – The traditional battlestaff training architecture is a collection of traditional (e.g., kinetic, EW, intelligence, etc.) M&S networks, protocols and software applications used to simulate key battlespace events and stimulate C4I systems and processes in use by the training audience. The USAF's ACE-IOS system can detect traditional effects of interest (e.g., kinetic damage to a communications capability) and pass those effects to the cyber range environment through the network guard. The traditional battlestaff training architecture is also responsible for receiving and correlating cyber effects of interest (e.g., network performance degradation, system failure) from the cyber range environment and degrading the applicable simulated system capabilities and/or passing the effect to the cyber emulation to degrade the corresponding training audience network-based service or workstation.
- **Cyber Emulation** – The cyber emulation is an accredited tool for emulating network and host cyber effects on training audience workstations that have been sensed from within the cyber range environment. The cyber emulation does not affect the underlying network, nor does it damage the affected workstation. For COATS, the Network Effects Emulation System (NE2S) Master Control Station (MCS) is responsible for receiving cyber effects from the traditional battlestaff training architecture and initiating the corresponding emulated cyber effect on the applicable training audience workstation. Using a remotely-accessible web interface, the NE2S MCS provides situational awareness and positive command and control of emulated cyber effects. An NE2S client application is installed on each workstation to be affected that must establish and maintain secure communications with the NE2S MCS in order for effects to be initiated. Effects can be instantaneously started, stopped or adjusted from the MCS for an individual workstation, a group of workstations, or all workstations. If secure communications are not established or maintained, existing effects will timeout, no new effects will be initiated, and all affected workstations will be restored to previous (unaffected) conditions.

> cyber emulation is an accredited tool for emulating network and host cyber effects

As depicted in Figure 2, COATS does not interface with or affect existing simulation-to-C4I interfaces used to stimulate the operational networks and systems in use by the training audience. COATS interfaces with M&S tools within simulation federations via the cyber DEM and affects operational workstations via the cyber emulation.

COATS USFK Deployment

The COATS architecture and associated technologies were deployed across the Continental U.S., Hawaii, and the Republic of Korea to support FY14/FY15 demonstration and training events with U.S. Forces Korea (USFK) and 7th Air Force (7 AF) during exercises Ulchi Freedom Guardian (UFG) 2014, Key Resolve 2015 and UFG 2015. The cyber range environment was provided by the USAF 90th Cyberspace Operations Squadron and used the Joint Information Operations Range (JIOR) and the network guard (RM plus ACE-IOS JIOR Broker) to share data over the Korea Battle Simulation Center (KBSC) Training and Exercise Network (KTEN) with ACE-IOS. ACE-IOS at the Korea Air Simulation Center (KASC) communicates with other M&S tools within the Joint Training Transformation Initiative + Korea (JTTI+K) federation (e.g., the Distributed Information Operations Constructive Environment) over KTEN as well as through a firewall to the NE2S MCS on the Combined Enterprise Regional Information Exchange System-Korea (CENTRIXS-K) network. The NE2S client software is deployed at USFK 7 AF to provide a contested training environment for the battlestaffs. A graphical depiction of this architecture is provided in Figure 3.

The COATS USFK deployment supports four generic vignettes that can be tailored and integrated into the exercise scenario and Master Scenario Event List (MSEL) as required. The four vignettes are:

- **Computer Network Attack (CNA)** – Live red CNA against virtual blue systems to demonstrate virtual host degradation effects on live operator workstations. See Figure 4 for additional details.
- **Physical Node Attack** – Constructive red kinetic attack on a constructive blue communications facility to demonstrate C2 disruption effects on live operator workstations.
- **Distributed Denial of Service** – Live red CNA on virtual blue systems to demonstrate virtual full-motion video degradation effects on live operator workstations.
- **Threat Network Degradation** – Live blue CNA on virtual red networks to demonstrate constructive system degradation on constructive red systems.

COATS FST Deployment

In March of 2016, COATS was demonstrated during a Fleet Synthetic Training (FST) event sponsored by the Office of Naval Research (ONR). FST events are computer-assisted exercises conducted using models and simulations to stimulate and represent real world command and control systems. The Navy Continuous Training Environment (NCTE) supports FST by combining interoperable shore-based and ship-embedded systems into a single, distributed simulation network. In FST RDT&E 16-1, ONR and the CWIC collaborated to introduce cyber degraded training for the first time. Cyber attacks were executed and detected within a cyber range environment, transmitted to NCTE, and presented to the training audience in the form of degraded services. Using the cyber DEM and capabilities provided by mission partners, this proof-of-concept demonstrated one avenue for fulfilling SECDEF and CJCS direction to include realistic cyber degraded training in service exercises and training. Vignettes included:

- **Compromised Common Operational Picture (COP)** – A simulated coalition maritime patrol aircraft was targeted for physical compromise and malware was loaded onto simulated C2 systems. Once airborne in the demonstration

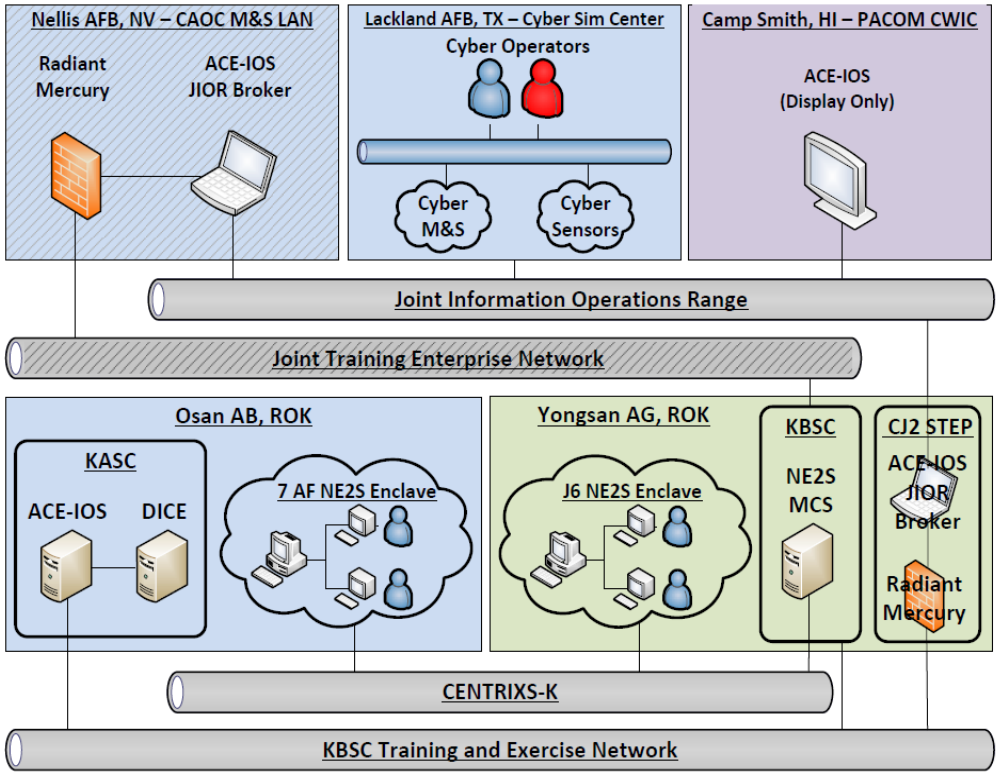


Figure 3. COATS USFK Deployment - *Source: Author*

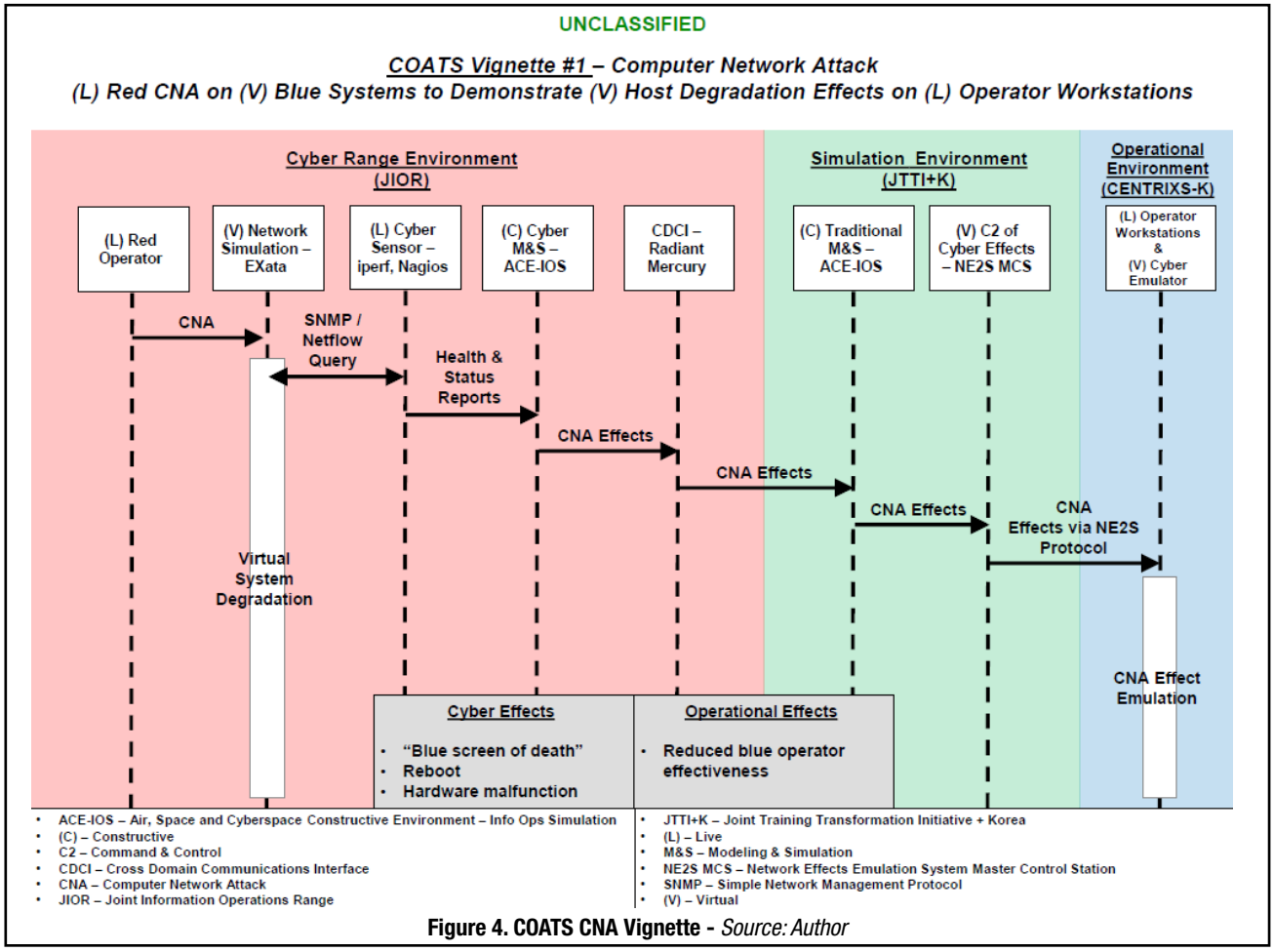


Figure 4. COATS CNA Vignette - *Source: Author*

scenario, data link track data was manipulated using messages based on the cyber DEM to degrade the COP and introduce doubt regarding position of hostile and neutral tracks.

- **Degraded Full Motion Video (FMV)** – A cyber attack within a portable cyber range environment targeted the FMV feed from a simulated Unmanned Aerial Vehicle (UAV) surveilling vessels of interest. Using the cyber DEM and NE2S, the display in the Coalition Maritime Operations Center was degraded, diminishing the ability to effectively identify and surveil shipping.

COATS I/ITSEC OBW Deployment

The COATS architecture and associated technologies were demonstrated at the 2015 and 2016 Interservice/Industry Training, Simulation and Education Conference (I/ITSEC). Operation Blended Warrior (OBW) was a cornerstone event of the conference integrating products and services of participants across the conference floor to demonstrate interoperability in a time-compressed demonstration. This LVC event was designed to represent a military exercise and demonstrate how integrated technologies can help commanders and exercise planners meet their training objectives. As lead for the cyber element of OBW, the CWIC introduced COATS to deliver cyber effects to the simulated Operations Center. Vignettes included:

- **Degraded FMV** – This vignette integrated a simulated UAV flying over simulated terrain with a cyber attack conducted within a cyber range environment. The attack was detected by COATS sensors, translated using the cyber DEM and sent to a workstation providing the FMV feed to the Distributed Training Center. NE2S installed on that workstation caused a simulated packet loss to the video feed rendering it unusable.
- **Radio Frequency Attack on Satellite Uplink** – Simulated transmission of interference of the FMV uplink to a simulated satellite was detected and translated into a cyber DEM-formatted message resulting in degradation similar to the network attack above.
- **Degraded Voice Over Internet Protocol (VOIP)** – Similar to the degraded FMV vignette, an attack in the cyber range, transmitted via COATS and cyber DEM, was interpreted by NE2S to simulate packet loss and render VOIP communications unusable until the attack was defeated.
- **Insider Threat** – Using a phishing feature in NE2S, a chat room interloper shared a link that resulted in degraded Operations Center workstations when selected by others in the chat room.
- **Kinetic Effects Integration** – As the finale of the degraded FMV vignette, the intelligence cell located the operating location of the cyber aggressors and a simulated tactical fighter aircraft kinetically destroyed the facility, restoring the FMV feed.

Lessons Learned

Key lessons learned from the planning, implementation, deployment and operation of COATS capabilities at USFK battlestaff exercises, service training exercises, and integration demonstrations are detailed in the following sections.

Planning

Planning for integrated cyber operations during a major exercise was the most significant and resource intensive challenge we experienced. Socialization and coordination of COATS activities was required across multiple organizations and throughout all levels of each organization (senior leader to action officer to technical support contractor). Past experiences with cyber training and exercises and a lack of understanding of the current state of the art often led to concerns about COATS and its potentially negative impact on the broader exercise objectives and training audience performance. As a result, an incremental approach was implemented that included multiple demonstration and test events to increase the battlestaff's level of familiarity and comfort with the technologies. Once the technologies were verified and approved, the details and procedures for how to integrate and command and control degraded cyberspace conditions in a battlestaff exercise were immature or non-existent. Exercise planning products and exercise control procedures had to be updated to include measures and controls for implementing and monitoring degraded cyberspace conditions and had to be integrated and synchronized with the overall exercise objectives, scenario, and MSELs.

Reluctance to accept risk in implementing cyber events is not unique to traditional exercises. While the nature of technical demonstrations such as FST and OBW lowers the hurdles for introducing cyber warfare, the real or perceived risk means planners must be prepared to convincingly advocate for inclusion of meaningful cyber events. This may result in cyber vignettes conducted on the periphery of, or in parallel with, traditional or primary demonstration objectives. Ultimately, cyber planners should be prepared with an alternate plan to demonstrate cyber effects that traditional warfighters can relate to. Exposure of leaders to cyber is the goal; savvy leaders will grasp the ramifications of potential direct cyber effects and will help shape future events to emphasize cyber and prepare their staff and subordinates to fight through a cyber attack.

Implementation

The implementation of COATS at USFK required the integration of existing cyber range environments, cyber and traditional M&S tools, and cyber emulations across disparate cyber, training and operational networks. This integration required the development of the cyber DEM, modifications to existing traditional M&S tools to become "cyber aware," and the use of the COATS network guard (RM and ACE-IOS JIOR Broker) to enable secure data flow between cyber ranges and simulation networks. Functionality and data flow were verified prior to each event as part of a Comprehensive Integration Test. The current implementation supports up to four generic vignettes that can be tailored and integrated into the overall exercise scenario and MSELs. Additional vignettes for different mission areas (e.g., Integrated Air and Missile Defense) are possible but would likely require additional modifications to traditional M&S tools to receive and realistically respond to the cyber effects represented within the cyber DEM. The risks and costs associated with the technical implementation of COATS at USFK were relatively low due to the reuse of existing capabilities and the straightforward integration strategy.

Deployment

The deployment of COATS technologies at USFK was most impacted by Information Assurance (IA) policies and procedures. Existing certification and accreditation products had to be reviewed or expanded before local authorities would approve installation and operation; approval via reciprocity was not an option. IA requirements for the simulation network (owned and administered by the KBSC) were different from those on the operational network (owned and administered by 8th Army's 1st Signal Brigade).

In the FST and OBW demonstrations, the cyber DEM proved to be a flexible framework for conveying cyber effects. With little or no previous exposure to COATS, proficient developers were able to quickly adapt the model and expand on messages pre-scripted for NE2S. They developed cyber DEM messages to generate new cyber events including generation of nefarious link tracks and were able to generate effects simulating network packet loss. This is an important aspect of the overall COATS vision for an architecture and model that can mature to meet evolving requirements for cyber degraded training.

Operation

The operation of COATS technologies was straightforward and was aided by the personnel and associated roles and responsibilities detailed in Table 1.

Reluctance to accept risk in implementing cyber events is not unique to traditional exercises.

Recommendations

The following recommendations are provided to assist current and future COATS sponsors, capability developers, users and maintainers with the successful development and employment of COATS and related capabilities.

Doctrine / Leadership / Policy

Joint Commanders must understand and direct their staffs to respond to existing SECDEF and CJCS requirements

Table 1. COATS Manning Plan - *Source: Author*

Role	Responsibilities	Qualifications	Location
Cyber Subject Matter Expert (SME)	» Monitor the execution and training audience response to all cyber MSELs, including COATS » Report results to the exercise control group » Report related issues to the COATS SME	Needs to be aware of COATS but does not need to be a COATS SME	Exercise control group / Cyber working group
COATS SME	» In coordination with the Cyber SME, monitor the execution of COATS-supported MSELs » Report COATS technical issues to the Cyber SME » In coordination with the COATS technician, monitor the status of COATS technologies	Must be a COATS SME; must understand exercise control group Tactics, Techniques and Procedures (TTPs)	Exercise control group / Cyber working group
COATS Technician	» Monitor and report the status of COATS technologies to the COATS SME » When requested by the COATS SME, troubleshoot and resolve technical issues	Must be a COATS technical SME	Various
NE2S Operator	» As requested by the Cyber SME, execute and monitor COATS-supported MSELs » Report technical issues to the COATS technician	Should be a trained, trusted agent from the supported command	Anywhere on operational network
ACE-IOS Operator	» As requested by the Cyber SME, execute and monitor COATS-supported MSELs » Report technical issues to the COATS technician	Must be an ACE-IOS SME; could be an additional duty for an existing position	Simulation center

and guidance for incorporating realistic cyberspace conditions into exercises. "Military campaign plans must fully incorporate the ability to operate in a degraded cyber environment; military forces must exercise and be able to conduct military campaigns in a degraded cyber environment where access to networks and data is uncertain" (Carter 2015). "The Combatant Commands and Services should reduce restrictions that prevent testing and training against realistic cyber threats, and perform "fight-through" events to demonstrate that their critical missions are resilient in contested cyber environments" (Gilmore, 2016).

Leaders must understand and accept the risks associated with degraded/denied cyberspace conditions in exercises and encourage their peers and subordinates to incrementally improve the quality and quantity of cyber play. Accordingly, organizations should not be criticized for negative performance impacts as a result of conducting operations in a contested training environment. The SECDEF provides this guidance on the topic:

"During the Cold War, forces prepared to operate in an environment where access to communications could be interrupted by the adversary's advanced capabilities, to include the potential use of an electromagnetic pulse that could disrupt satellite and other global communications capabilities. Commanders conducted periodic exercises that required their teams to operate without access to communications systems. Through years of practice and exercise, a culture of resilience took root in the military and units were ready and prepared to operate in contested environments.

Since the end of the Cold War, however, a younger generation has grown increasingly more accustomed to an environment of connectivity. The generation of military men and women that grew up since the end of the Cold War have had near constant access to information and communications, and the information revolution has led to a more agile and globally adaptive force. In the face of an escalating cyber threat, the lessons of the previous generations must now be passed down. The Defense Department must be able to carry out its missions to defend the country. Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations" (Carter 2015).

cyber emulation is an accredited tool for emulating network and host cyber effects

Training

Exercise program strategies, plans and products must be updated to increase the quality and quantity of cyber play in accordance with an organization's concept and operational plans. Examples include exercise concepts, training objectives, scenarios, MSELs, exercise control group organization and procedures, and after action review/lessons learned procedures. An incremental approach is recommended to increase the leaders' and the staff's level of familiarity and comfort with any new technologies, processes and procedures. Consider conducting a small-scale table-top exercise or similar construct to practice key process and procedure changes prior to implementation.

Materiel

Additional materiel research, development, test and evaluation is necessary to expand and mature the current COATS technologies to better address the required mission areas and improve the level of interaction, resolution, and command and control of the integrated training environment as follows:

- Cyber Effects Resolution – The ability for cyber sensors, models and effects to interact with specific applications, services, ports and protocols.
- Virtual Network Generation – The ability to rapidly scan, generate, correlate and share network, system, and application deployment and configuration data between cyber ranges, traditional simulation architectures, and cyber emulators.
- Network Defender Training – The ability for network defenders to protect, detect,

react and restore network operations based on feedback from and interaction with COATS sensors, models and effects.

- Threat Networks – The ability for COATS sensors, models and effects to realistically represent and degrade opposing force systems and networks.
- Cyber Range Command and Control – The ability to integrate and synchronize the management of cyber range environments with traditional simulation architectures (e.g., start/stop/pause/resume, checkpoint/restore, database synchronization, etc.).
- Cyber DEM – The ability to support additional mission sets (e.g., IAMD) and to be easily applied to existing DoD M&S standards.

Summary

This article introduced the COATS architecture and how it can be used to meet SECDEF and CJCS requirements for incorporating realistic cyberspace conditions into battlestaff training and exercises. The article also discusses lessons learned from the employment of COATS during three USFK exercises, two iterations of OBW at I/ITSEC 2015 and 2016, and a proof-of-concept demonstration of COATS integrated into a Navy FST event. Included are recommendations for future development and employment. Ideally COATS would be combined with other types of cyber training solutions (e.g., scenario injects and red teams) to provide a multi-resolution approach to integrated cyber training such as we see with the combination of LVC technologies used for traditional military operations training. It will take time for leaders and their staffs to become familiar and comfortable with cyber training capabilities such as COATS and it will take time for exercise programs to fully integrate cyber training objectives, processes and procedures into their existing products. COATS offers a near-term, verified method to synchronize and deliver realistic cyber effects to the entire battlestaff – cyber for all.

- USFK KBSC, Joint Cyber Center, J635
- 7 AF KASC, A3, A6, 607th Air and Space Operations Center
- USAF 90th Cyberspace Operation Squadron
- USAF 453rd Electronic Warfare Squadron
- Naval Air Warfare Center Training Systems Division
- Johns Hopkins University Applied Physics Laboratory

Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations

Acknowledgements

USPACOM would like to thank the following COATS sponsors, performers, and supporters for their dedication and expertise:

- Office of the Undersecretary of Defense, Acquisition, Technology and Logistics – Dr. Steven King and staff
- DMSCO – Mr. Jesse Citizen and staff
- Office of the Director, Operational Test and Evaluation
- Joint Staff J7

REFERENCES

[1] Carter, A. (2015). The DoD Cyber Strategy. Page 17.

[2] Gilmore, M. (2016). Director, Operational Test and Evaluation FY 2016 Annual Report. Page 444 (Cybersecurity)

[3] Goldfein, D., (2014). CJCSI 3500.01H Joint Training Policy for the Armed Forces of the United States. Page D-7.

[4] Morse, K., & Drake, D., Wells, D., Bryan, D. (2014). Realizing the Cyber Operational Architecture Training

[5] System (COATS) Through Standards. 2014 Fall Simulation Interoperability Workshop. Page 7.

ABOUT THE AUTHORS

Dr. David "Fuzzy" Wells is the Director of the U.S. Pacific Command's (USPACOM) Cyber War Innovation Center (CWIC) and the Technical Lead for COATS. A retired Air Force (AF) officer, his past assignments include: Chief Scientist for Research and Development at the Joint Warfare Analysis Center; Chief of Ops Assessment at AF Central Command's Combined Air & Space Ops Center; Chair of Ops Research Working Group, Director of Modeling & Simulation (M&S) Education and Assistant Professor of Computer Science at the U.S. Air Force Academy; AF M&S lead for U.S. Joint Forces Command's Millennium Challenge experiment while at the AF Agency for M&S; and Prime Warrior Course Director and AF lead for the Prairie Warrior exercise while at the AF Wargaming Institute. He has served as exercise designer and senior controller for battlestaff training exercises worldwide. He was the first AF officer to obtain a Ph.D. in Modeling, Virtual Environments and Simulation from the Naval Postgraduate School. He also earned the first M.S. in Modeling & Simulation from the AF Institute of Technology. He is a Certified Modeling & Simulation Professional Charter Member and a National Modeling & Simulation Coalition Plankholder.

Derek Bryan has provided direct support to the USPACOM J81 – Joint Innovation and Experimentation program since 2005. In this role he is responsible for the research, testing, and assessment of innovative solutions to USPACOM capability gaps. Mr. Bryan is currently providing project management and engineering support to the CWIC and the COATS project. Mr. Bryan has a B.S. in Computer Science from James Madison University and an M.E. in Modeling and Simulation from Old Dominion University.


ADVANCED PERSISTENT THREAT (APT)
192.168.1.100
192.195.226.
192.195.157.244
192.195.188.126
192.195.169.12
192.195.147.163

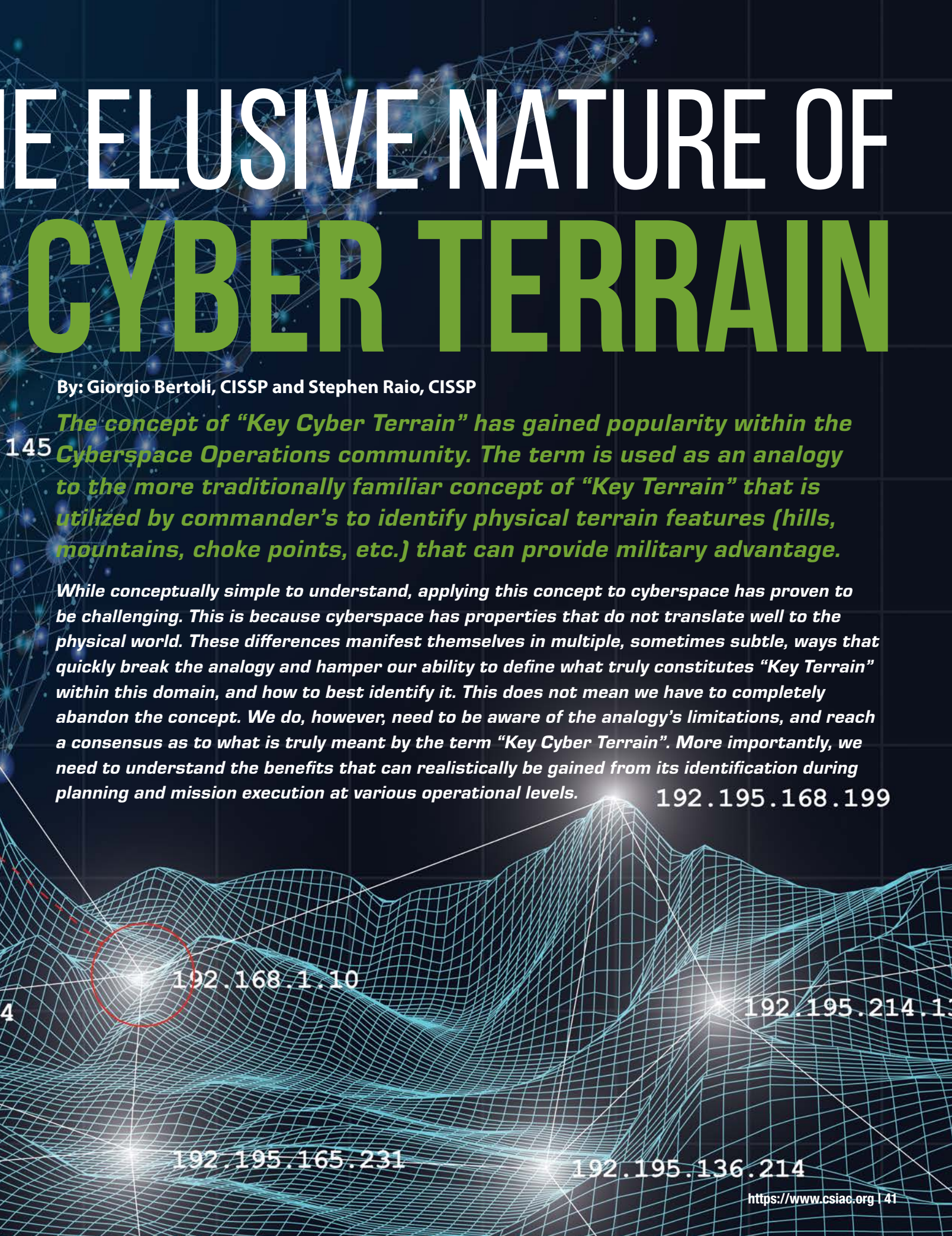
TH
KEY

IE ELUSIVE NATURE OF CYBER TERRAIN

By: Giorgio Bertoli, CISSP and Stephen Raio, CISSP

The concept of "Key Cyber Terrain" has gained popularity within the Cyberspace Operations community. The term is used as an analogy to the more traditionally familiar concept of "Key Terrain" that is utilized by commander's to identify physical terrain features (hills, mountains, choke points, etc.) that can provide military advantage.

While conceptually simple to understand, applying this concept to cyberspace has proven to be challenging. This is because cyberspace has properties that do not translate well to the physical world. These differences manifest themselves in multiple, sometimes subtle, ways that quickly break the analogy and hamper our ability to define what truly constitutes "Key Terrain" within this domain, and how to best identify it. This does not mean we have to completely abandon the concept. We do, however, need to be aware of the analogy's limitations, and reach a consensus as to what is truly meant by the term "Key Cyber Terrain". More importantly, we need to understand the benefits that can realistically be gained from its identification during planning and mission execution at various operational levels.



Introduction

"**Key Terrain**" is defined as "**Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 2-01.3)**" [1]. The value of terrain in support of defensive and offensive military operations has been known for millennia[1]. In a defensive context, for example, narrow ingress passageways can be used to mitigate a force with superior numbers. From an offensive perspective, avoiding terrain that hampers movement and using land features to protect your flank can significantly improve mission success [2]. The ability to identify such terrain features within the operational environment allows commanders to more effectively plan and tailor their efforts. To simplify some of the complexities of cyberspace, we attempt to make analogies to the physical world that allow us to apply familiar doctrinal processes. The concept of "Key Terrain" is one such construct that has manifested throughout the community as "Key Cyber Terrain" or "Key Terrain within cyberspace" [3] [4].

To simplify some of the complexities of cyberspace, we attempt to make analogies to the physical world that allow us to apply familiar doctrinal processes. The concept of "Key Terrain" is one such construct that has manifested throughout the community as "Key Cyber Terrain" or "Key Terrain within cyberspace" [3] [4].

A common theme that seems to be shared amongst all practitioners, is that "Key Terrain" should be directly linked to mission objectives. This is relatively intuitive given that terrain that is advantageous to one side for some operational scenario is obviously a disadvantage to the other. Another agreed upon attribute is that its value is temporal; coupled with the duration of a mission. For instance, fighting from an elevated position (high ground) is beneficial for a number of reasons. Holding higher ground provides an elevated vantage point with a wider field of view. Soldiers fighting uphill will move more slowly and tire more quickly, and so forth. However, depending on the timeframe, seizing the high ground is not always advantageous. If an opposing force has the time and capacity, they can surround a well-entrenched adversary, cutting off resupply and essentially just "wait them out"[2].

Applying both of these requirements to "terrain" within cyberspace seems straightforward. When executing a certain military operation, only portions of this virtual domain will be important or advantageous; changing over time based on mission timespan or as the mission evolves. But, what within cyberspace equates to "terrain"? How do we identify what aspects are advantageous in support of a specific mission? Even more troubling, how do we even scope a "mission"? Defining a mission too broadly, (e.g. maneuver to, seize, and secure objective TANGO), quickly renders the problem of identifying all essential cyberspace resources intractable [5]. Conversely, define a mission too granularly (e.g. fuel my vehicle now) makes it easy to bound, but causes excessive vacillations on what is important as we switch across a large set of tiny concatenated tasks.

These open questions are further complicated by the fact that warfare within the Cyberspace Domain has undeniable dissimilarities from the more traditional physical domains of land, maritime, air and space [6] [7]. These differences have proven to be of sufficient complexity to keep "Cyber Key Terrain" an elusive concept that is yet to be consistently defined or fully understood.

"Cyber Key Terrain" an elusive concept that is yet to be consistently defined or fully understood.

1 Sun Tzu, when discussing the importance of terrain in warfare stated: "We may distinguish six kinds of terrain, to wit: (1) Accessible ground; (2) entangling ground; (3) temporizing ground; (4) narrow passes; (5) precipitous heights; (6) positions at a great distance from the enemy."

2 As an example, in Battle of Jieting of the Three Kingdoms period of China, Shu Han forces occupied a hilltop, which opposing forces soon surrounded, isolating them from supplies and reinforcements. As a result, the Shu forces were defeated [https://en.wikipedia.org/wiki/Battle_of_Jieting].

Analogy Breakdown

This article presents multiple aspects of cyberspace, and associated challenges, that are hampering our ability to apply the concept of "Key Terrain" within the domain. These include: differences in what constitutes terrain and associated fundamental properties, inconsistences in definitions, challenges pertaining to the visualization and understanding of cyberspace, incongruence in the identification of mission critical systems vs. overall security risks, difficulties in bounding the problem when applying the concept to a complex system, and nonequivalence when attempting to utilize the concept to prioritize resources.

What is "terrain" in cyberspace

Before we can begin any discussion on the identification of "Key Cyber Terrain" we must first answer the more fundamental question of what is "terrain" within this virtual man-made environment. Surprisingly, not much has been written on this topic. Most existing literature seems to operate on the assumption that cyberspace terrain is simply the systems, devices, software and interconnections that constitute cyberspace itself. Raymond et all [4] are among the few that attempt to provide a formal definition:

> *"The systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace"*

This characterization seems to follow the philosophy that terrain within cyberspace is basically anything and everything that makes up, or is a part of, the domain.

Comparing to the physical world, terrain is defined as:

> *"A stretch of land, especially with regard to physical features[3]".*

While military doctrine does not formally expand on this definition, in practice "Key Terrain" is understood to include both natural land features as well as man-made objects, such as bridges, buildings, or more strategic

3 https://en.oxforddictionaries.com/definition/terrain

elements such as ports and cities, which can also provide military advantage.

Comparing these two definitions, one can already see some significant differences. Within the physical world, terrain is a finite subset of the domain. For instance, there is a clear differentiation between what is a terrain feature vs. what is a military asset (i.e. a valley or a bridge vs. a tank or a plane). Within cyberspace, this distinction no longer exists. The ability to easily differentiate between terrain features vs. assets is lost. The provided definition even includes cyber personas, in essence encapsulating virtual individuals as part of the terrain landscape. This fundamental expansion of what constitutes "terrain" within cyberspace, results in numerous ambiguities and interdependencies, which make identification of "Key Terrain" within it very challenging.

Inconsistences in defininng "Key Cyber Terrain"

No official doctrinal definition of "Key Cyber Terrain" exits. To bypass this discrepancy, the term "Key Terrain within cyberspace" is gaining popularity. In this context, the well understood definition for "Key Terrain" is directly applied to cyberspace equivalent to the other domains. While this approach appears reasonable, as previously discussed, it fails to acknowledge that "terrain" in cyberspace is much broader in context.

Regardless of semantics, the concept of "Key Cyber Terrain" is most often used to signify the physical and logical elements within cyberspace that are critical enablers for the successful execution of a mission[4][8]. Within this context, some have postulated that "Key Cyber Terrain" is simply a subset of the broad categories of hardware and software components that are essential for the execution of a particular mission. These can include such things as physical and transport layer infrastructure (e.g. undersea cables, service providers), computing and data centers, or key services (e.g. Domain Name Service), to name a few [3] [4]. Others have equated "Key Cyber Terrain" to critical capabilities or assets that support a specific type of military operation (e.g. Fires => AFATDS[5] or Missile Defense => BMDS[6]) [9] [5]. Both approaches are limited in their usefulness [7]. In the first case, "Key Cyber Terrain" becomes too abstract or diffuse of a concept, quickly extending beyond the area of operations for all but the most strategic of commands. In the latter, "Key Cyber Terrain" is oversimplified to mean a specific mission enabling application or system. This view of terrain does not have the same context as its physical counterpart, and is in essence equivalent to claiming a tank or a ship (regardless how important it is to the mission) is "Key Terrain". Physical terrain does not in itself provide a capability. It provides military advantage, enhancing the effectiveness of capabilities you already possess, or tactics you employ. If the physical components of systems such as AFATDS or BMDS are not "Key Terrain" in the land domain, then why should their logical representations within cyberspace be?

> "Key Terrain" is understood to include both natural land features as well as man-made objects, such as bridges, buildings, or more strategic elements such as ports and cities, which can also provide military advantage.

Differences in the fundamental properties of "terrain"

Terrain features in the physical world have intrinsic properties that are well defined and understood. Mountains and swamps are hard to cross, dense vegetation provides obscurance, and hilltops provide a better field of view. Each of these properties is immutable. Their value to a military operation is only dependent on their geographical position relative to the intent and duration of a particular mission.

It can be argued that certain devices or services within cyberspace provide functions that imbues them with some fundamental characteristics that are comparable to the examples provided above. For instance, a router by design has access to a large amount of network traffic. The more principal the router (core backbone, country gateway, etc.) the more traffic it can "see". So are routers in cyberspace then analogous to high ground, providing varying levels of increased visibility?

The analogy does seem to be intuitively sound, but there are still some fundamental differences. Though a router does provide the ability to observe more network traffic, this does not really translate to the same type of visual awareness that a hill can provide. This is because network traffic flows are comparatively much more complex. For instance, their point of origin and destination are at times obfuscated, and can extend well outside a commander's area of interest without any simple mechanisms for determining which are of relevance (especially at lower echelons).

More importantly, current operational policies and rules of engagement limit how such cyberspace terrain can be leveraged. A tactical commander does not have the authority to commandeer a network router[7] as they do a hilltop within their Area of Operation. This is a core fundamental difference in the analogy that is often overlooked. As discussed in [4], "Key Terrain" in kinetic warfare spans tactical, operational, and strategic levels, but it is most commonly applied at the tactical edge. At these lower echelons, a commander can readily take advantage of terrain features within their purview to the benefit of the mission. Within cyberspace, this model is reversed. The steep Intel requirements necessary to understand

4 You may have noticed, that this explanation of what is meant by "Key Cyber Terrain" does not equate to the definition of "Key Terrain" that was previously referenced. Terrain that provides a "marked advantage" is not the same as a "critical enabler" for mission execution.

5 AFATDS: Advanced Field Artillery Tactical Data System

6 BMDS: Ballistic Missile Defense System

7 Policy discussion are beyond the scope of this document. It can be speculated that in the future existing Cyberspace Operations restrictions will be relaxed, however, there will still be significant implications (e.g. potential collateral damage, laws, force structure and capability requirements, etc.) that will still have to be considered when operating within this domain.

cyberspace, coupled with its geographical ambiguities and legal restrictions, make the concept hard to apply at the tactical level without significant higher echelon, or even strategic level support.

Challanges with visualizing and understanding cyberspace

When identifying "Key Terrain", a tactical commander can look at a map and readily recognize land features that can provide advantage or disadvantage for a particular maneuver operation. These structures can be within friendly, neutral or adversary space. They may be currently uncontested, or under direct enemy control. While cyberspace has many of these same properties, they are much harder to understand and visualize. For instance, determining if an adversary controls some device or service within cyberspace can be difficult to ascertain as it does not necessitate the physical occupation of some geographical region [4].

In some respect, the concept of "Key Cyber Terrain" highlights some of our current capability gaps with the domain. For example, logically mapping all of cyberspace within an area of interest is highly challenging from a purely technical perspective[8]. In addition, features within cyberspace that may be potentially relevant to a military operation cannot be easily mapped or confined a tight geographic boundary. Such limitations significantly hamper a commander's ability to identify what portions of cyberspace, within their purview, are important to their mission.

Because of these barriers, we often artificially limit the scope of "Key Cyber Terrain" by primarily looking inward, to military systems and networks ("Blue" space) that are under a commander's direct control. Even this, however, has proven hard to do[9], and thus, often deteriorates even further to the identification of mission critical assets. Applegate et al. [7] states the following on the matter:

> *"...defining and protecting critical assets should not be confused with identifying "Key Terrain". Understanding how the identification of critical assets shapes the identification of key terrain during a mission is important to the success of our cyberspace planners. This process allows planners to prioritize critical assets, create a Critical Asset List, determine which assets should be defended, develop a Defended Asset List, and then identify key terrain in relation to these assets and mission objectives."*

a Critical Asset List, determine which assets should be defended, develop a Defended Asset List, and then identify key terrain in relation to these assets and mission objectives.

While this statement takes a strong position on how the identification of critical assets is not equivalent to "Key Terrain", it does little to explain what "Key Cyber Terrain" is. One can even argue that this assertion makes it hard to see what additional value the concept provides beyond everything that was previously listed.

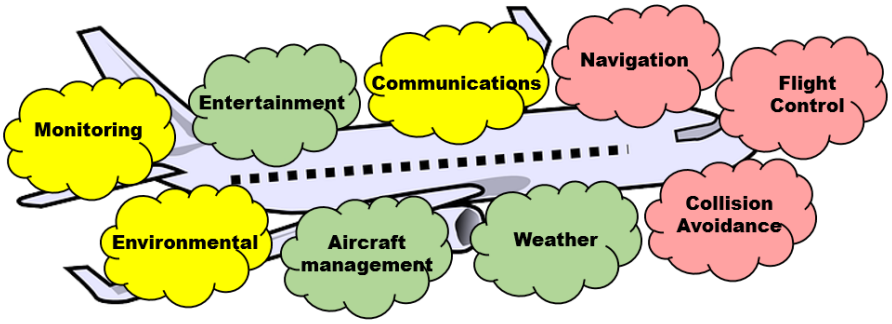


Figure 1. Example aircraft control systems, color coded by importance during flight (red = high, yellow = moderate, Green = low) - *Source: Author*

Incongruities between the criticality of a system vs. overall risk

From a Defensive Cyberspace Operations (DCO) perspective, limiting the concept of "Key Cyber Terrain" to mean just critical, or high value, systems and service (as proposed in [5] [9]), can actually provide a false sense of security. The criticality of a system to a specific mission does not necessarily equate to what constitutes its highest security risk [10]. This is especially true when dealing with a complex system with intricate interdependencies.

For example, consider a modern commercial aircraft as depicted in figure 1. This airplane contains multiple control systems. Clearly, some are more important than others during flight. These subsystems, however, are not fully independent. For instance, collision avoidance must be able to communicate with flight control to redirect the aircraft in an emergency. Flight control must be able to communicate with navigation to maintain heading, and so on. These interdependencies are so pervasive, that most aircraft are equipped with a variety of common communication buses and protocols[10] that interlink almost all such subsystems in a standardized manner. From a computer security perspective, this renders their relative functional importance potentially irrelevant. In May of 2015, cybersecurity consultant Chris Roberts claimed to have been able to

8 The many technical challenges associated with the logical mapping of cyberspace is the subject of numerous scholarly articles.

9 For example, the ability to map networking infrastructure and services to specific mission objectives has proven to be very technically challenging [5].

10 Avionics data interchange standards for modern aircraft include: ARINC 429, ARINC 629, MILSTD 1553, MIL-STD 1773, CSDB and ASCB.

take control of an aircraft's engines via the onboard entertainment system and cause the plane to climb during flight [11]. This was later debunked, as the entertainment system within the aircraft fortunately did not have any connectivity to flight control systems [12]. But, had there been[11], would anyone have had reason to consider the entertainment system as critical to flight? In the now infamous Target Corporation Point-of-Sales compromise that resulted in 10's of thousands of stolen credit cards[12], can anyone within Target's senior management truly be blamed for not having considered connectivity to a low priority, 3rd party, refrigeration contractor as "Key Terrain" within their enterprise network[13]?

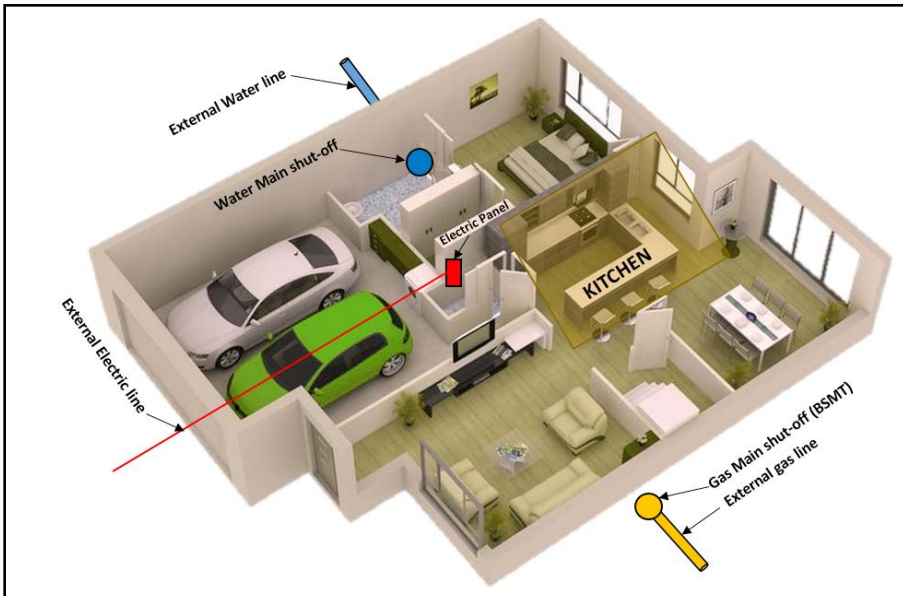


Figure 2. Model of a typical home - *Source: Author*

Difficulties in bounding the problem within a complex system

Another fundamental property of physical terrain is that they are "simple" closed systems bound in three dimensional space. A hill, after all, is just a hill, and as such, possesses certain "hilliness" attributes that can be beneficial or detrimental depending on the use case. It is, in large part, this simplicity that allows a tactical commander to readily identify "Key Terrain" within a traditional military context. However, when the concept is applied to a complex system, the problem can rapidly become intractable. To better illustrate this, consider the following scenario:

> *Your mission is to cook dinner tonight in the home depicted in figure 2. You have all the ingredients you need within the kitchen, and you identify the stove and the oven as critical systems you must maintain control of and keep functioning.*

Given this relatively simple situation, what is the "Key Terrain"? Clearly the kitchen itself is of critical mission importance. We can ensure we block off and guard all physical avenues of approach to this space relatively easily, but is that sufficient? As it turns out, the stove runs on natural gas, the oven on electricity, and we also need water (a critical ingredient for the planned meal). Gas and water shut-off valves, and the electrical panel, are in different rooms within the house, so we need to protect them as well. What about the gas, power and water lines that run external to the home? What about the power distribution center that serves the neighborhood? Do I need to protect that as well? What about the water reservoir that serves the town[14]?

When applied to a complex system, what comprises a critical resource is hard to bound; continuing to expand further and further away from what is in our direct control as dependencies branch outwards[15]. The situation can be made even more complicated by simply increasing the mission's execution time. For instance, what if the mission was to cook dinner every night for a month? Now we would also need to worry about obtaining resupplies, and ensure all the things that enable us to procure and transport them also remain available to us.

Unfortunately, most elements within cyberspace are, or are part of, a complex system that is not encapsulated within three dimensions, but rather some potentially uncountable number. This complexity, as illustrated by this simple example, manifests as a number of interdependencies that hamper our ability to bound the critical resources essential for mission success, or to identify aspect of the environment that may offer some advantage.

Nonequivalence in the ability to prioritize resources

One of the desired benefits obtained from the identification of "Key Cyber Terrain" is an ability to focus available resources on what is most important or advantageous for a mission's success. Within the more traditional physical domains, this trade-off analysis occurs almost naturally. When a commander identifies "Key Terrain" features they want to either defend or obtain control of, anything that remains are by default portions of the operational environment that, if necessary, they would be willing to cede to the adversary. This same tradeoff is not as clear when working with complex systems, as is the case for practically all cyberspace operations.

For example, let us revisit the scenario presented in section II.F. To truly guarantee mission success, we need a way of encapsulating everything we require to accomplish the mission into a closed self-

11 The presence of a communication path that may allow such an attack is a point of some contention. According to [12], some newer aircraft may allow for some two-way communications between such systems.
12 http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/
13 This question is somewhat rhetorical. The answer is of course yes, and multiple top target executives were fired because of this incident, but not because they did not properly identify their "Key Cyber Terrain". More on this in section III.
14 You may have noticed, that for this example, we have once again devolved to equating "Key Terrain" to mission critical resources. This same inclination often occurs when planning cyberspace operations; especially those that are defensive in nature.
15 [7] Argues that a unit should only focus on what is within their span of control and rely on higher echelons for the rest. This is a fair point, but it does still have some significant implications. For instance, mission planning (even for relatively simple missions) would necessitate extensive cross echelon coordination and resourcing.

contained system. But, even if we devise some means where we can cook dinner in the kitchen completely segregated from any external need (I have an electric generator for the oven, I stored enough water for my needs, I have a portable gas canister for my stove), does this mean we are willing to ignore all other things that are not currently essential? For instance, are we willing to let an adversary steal the cars from the garage because we do not need them at this time? Likewise, does identification of "Key Terrain within cyberspace" imply that we are willing to deviate network security focus and/or resources in a manner that can potentially allow an adversary to compromise other network systems that are not directly supporting the current mission[16]?

"Mission Aware Network Architecture" would allow for the automated tracking of data flows and system interdependencies to facilitate this mapping process

Re-Interpretation of the Concept

The previous section has identified several challenges associated with trying to directly apply the concept of "Key Terrain" to cyberspace. In summary, as currently defined, terrain within cyberspace encompasses all things that constitute the domain. As a result, it is difficult to differentiate between "terrain" elements that provide advantage and individual assets or capabilities that are important for the execution of a specific mission. Practically all systems within cyberspace are complex in their function and often possess multiple external dependencies. As such, it is not enough to protect what we identify to be mission critical systems. We also need to consider all the data sources and communication links such capabilities rely on to function, and ensure those too maintain availability and data integrity. Even more problematic, any existing communication or access path to a system can serve as an attack vector with potentially greater security risk. If the mission is a prolonged campaign, then we would also need to protect all the logistics systems necessary for sustainment and resupply. And, even if we could do all these things, this does not imply that we can deviate resources away from other systems in a manner that may make them more susceptible to (or us less aware of) their potential compromise. Expanding to more offensive operations, which have to consider both civilian and adversary cyberspace networks and capabilities that are outside our direct control, makes these challenges even more pronounced.

This all leads to the inescapable conclusion that the concept of "Key Cyber Terrain" needs to be re-interpreted to deal with the complexities of the domain. A simplistic, but clearly sub-optimal, approach could just entail a re-definition of the term. For instance, if we indeed wish to equate "Key Cyber Terrain" to mean "Mission Critical Cyber Assets" (across blue, gray and red cyberspace), then we should clearly state this in doctrine, and then ensure we understand and agree on its use cases, benefits, and limitations.

A more interesting approach, is in the realization that "Key Cyber Terrain" may not necessarily be something within cyberspace that you identify, but rather something that must be created. Cyberspace is, after all, a virtual man-made domain. It is therefore reasonable to assume that "Key Terrain" within it may not naturally emerge, but must instead be explicitly architected within it[17]. In our previous aircraft example, having the ability to decouple individual subsystems from each other did allow for the identification of more important functions during flight. Even in our "cooking" example, we were able to devise a means to negate the need for certain critical mission resources that were outside our direct control. Achieving this, however, is not a trivial matter. Such segregation of functionality has to be explicitly designed within a system's architecture, through well-defined boundaries and interfaces that guarantee certain behavioral properties and protections, which are then enforced in implementation. As an example, [5] describes the challenges associated with mapping a mission to its required network resources. They even postulate that it may be impossible to do so with high fidelity within existing networks. However, they do hypothesize that establishment of a "Mission Aware Network Architecture" would allow for the automated tracking of data flows and system interdependencies to facilitate this mapping process. Given we cannot start from scratch and completely redesign all Army networks, we can begin by investing resources to obtain a much more detailed understanding of our networks as they exist today. If we can fully enumerate all interdependencies between systems and mission sets, we can then attempt to define and enforce strict boundary controls between core components, potentially creating "Key Cyber Terrain" in the process.

A last point for consideration is that perhaps, as the proverb says, the journey is more important than the destination. Application of the OCOKA[18] process to cyberspace as explained in [4] [14], appears in itself to be highly beneficial. By following this process in a methodical manner, the end state is that we have conducted a fairly detailed mission capability, threat, and risk assessment. Subsequent studies of the previously discussed Target attack have revealed many ways the company could have prevented the compromise from happening [13] [10]. None, however, relied directly on the concept of identifying "Key Terrain within cyberspace". Instead, they champion the institution and application of a comprehensive risk management process that, much like the OCOKA model, allows security experts and managers to systematically analyze their entire enterprise network and identify all potential security risks and weaknesses. Somewhere during the execution, or at the conclusion of such an analysis, we may be able to point to certain aspects of the

16 The answer to this question is clearly "no", but this does then imply that the usage of "Key Terrain" within cyberspace is not equivalent to its usage within the physical domains.

17 This can work well from a Defensive Cyberspace Operations perspective where we have the ability to define the architecture of our networks; a luxury we most often do not have within gray and red operational spaces.

18 OCOKA: Observation and fields of fire, Cover and concealment, Obstacles, Key or decisive terrain, Avenues of approach. http://www.armystudyguide.com/content/army_board_study_guide_topics/survival/ocoka.shtml

network which we deem to be "Key Cyber Terrain", but in reality, it was the application of the process that provided most of the benefit.

Further Research

We acknowledge that this article does not provide definitive answers to the fundamental question of what is "Key Cyber Terrain", or how to identify it. While we have made a few key observations and recommendations, we do agree that much more remains to be done. The intent of this article was to clearly articulate the fundamental properties of cyberspace that are preventing us from being able to readily apply the analogy. It is hoped that this will enlighten, and inspire continued conversation and research on the topic.

In the process of writing this article, what became increasingly clear is that we lack concrete use cases. Creating a set of detailed scenarios from which we can then attempt to identify "Key Cyber Terrain" as part of a well-defined process will be highly beneficial. Scenarios should be varied to include direct support to a tactical maneuver or engagement, as well as more strategic pre-phase three operations[19]. Scenarios should also include both defensive and offensive components. A final interesting observation, is that we have a propensity for applying the concept of "Key Cyber Terrain" across operational domain boundaries. In other words, we most often want to know how cyberspace operations can support traditional physical mission sets. It would be interesting to see if any of the challenges that have been presented in this document are alleviated when attempting to apply the analogy to military operations within cyberspace itself.

As part of our continued research within this technology space, we plan on developing some of these described use cases for further study. Attempting to apply the concept of "Key Cyber Terrain" to a well-defined and tangible set of missions should provide a valuable data corpus to help resolve some of the ambiguities that are currently stifling our efforts. Perhaps then, "Key Cyber Terrain" may cease to elude us.

19 The six phases of military operations are defined in Joint Publication 3-0.

REFERENCES

[1] Department of Defense, "DOD Dictionary of Military and Associated Terms," Defense Technical Information Center, 2017.

[2] J. Major Harry D. Scott, "Identification of Decisive Terrain," School of Advanced Military Studies, Fort Leavenworth, Kansas, 1993.

[3] J. R. Mills, "The Key Terrain of Cyber," Georgetown *Journal of International Affairs*, pp. 99-107, 2012.

[4] D. Raymond, G. Conti, T. Cross and M. Nowatkowski, "Key Terrain in Cybersapce: Seeking the High Ground," in *6th International Conferenece of Cyber Conflict*, 2014.

[5] S. A. E., K. M. C. and Z. J. R., "Cyber Network Mission Dependencies," MIT Lincoln Laboratory, Lexington, MA, 2015.

[6] G. L. D. W. U. (Ret.), "CYBERSPACE – The Fifth Operational Domain," *IDA Research Notes*, 2011.

[7] S. D. Applegate, C. L. Carpenter and D. C. West, "Searching for Digital Hilltops: A Doctrinal Approach to Identifying Key Terrain in cyberspace," *Joint Force Quarterly (JFQ)*, vol. 84, no. 1st Quarter, pp. 18-23, 2017.

[8] I. BG George J. Franz, *Effective Synchronization and Integration of Effects Through cyberspace for the Joint Warfighter*, US CYBER COMMAND, 2014.

[9] M. B. T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly (JFQ)*, vol. 73, no. 2nd Qrt, pp. 12-19, 2nd Qrt 2014.

[10] T. Radichel, "CASE STUDY: Critical controls that could have prevented Target breach," SANS institute, 2014.

[11] E. Perez, "FBI: Hacker claimed to have taken over flight's engine controls," CNN, 15 05 2015. [Online]. Available: http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/. [Accessed 05 04 2017].

[12] K. Zetter, "Is it possible to hack commerical aircraft?," WIRED, 26 05 2015. [Online]. Available: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/]. . [Accessed 05 04 2017].

[13] M. Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet, 02 02 2015. [Online]. Available: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/. [Accessed 05 04 2017].

[14] D. Hobbs, "Application of OCOKA to Cyberterrain," White Wolf Security, Lancaster, PA, 2007.

ABOUT THE AUTHORS

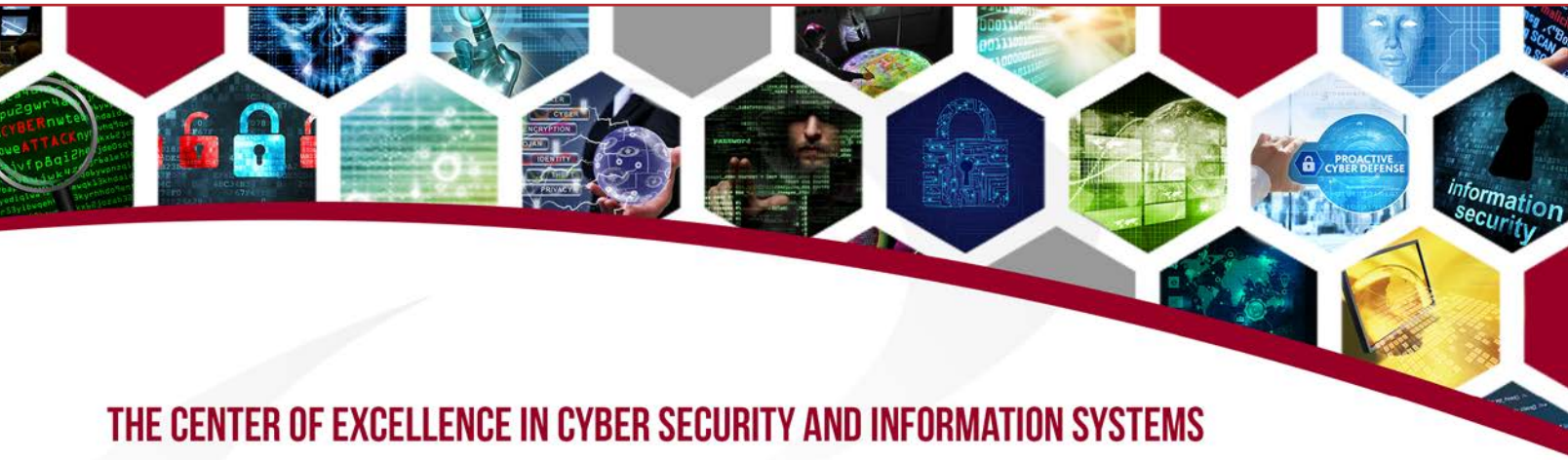
Mr. Giorgio Bertoli works for the US ARMY Intelligence and Information Warfare Directorate (I2WD), Communications-Electronics Research Development and Engineering Center (CERDEC), US Army Research Development and Engineering Command (RDECOM), where he is currently serving as Senior Scientific technology Manager (SSTM) of Offensive Cyber Technologies and Chief scientist.

With 25 years of federal service, Mr. Bertoli has extensive government experience in the areas of CYBER, Electronic Warfare, and military tactics both as a civilian and as a former active duty soldier. Mr. Bertoli's primary research areas include the development of advanced Electronic Warfare (EW), Computer Network Operations (CNO), CYBER and Quick Reaction Capability (QRC) technologies. Mr. Bertoli is also a highly proficient programmer in several computer languages, and is a subject matter expert in the area of Evolutionary Programming and AI/ML.

Mr. Bertoli has a Bachelor's and Masters Degree in Electrical Engineering from the New Jersey Institute of Technology, and a second Master's Degree in Computer Science from the University of Massachusetts Amherst. Mr. Bertoli is also a Certified Information Systems Security Profession (CISSP). During his 6 and a half year Military career, Mr. Bertoli served as a combat Engineer and was stationed in Germany, Ft Bragg NC, and Korea as well as being deployed as part of operation Desert Shield and Desert Storm.

Stephen Raio is an Army civilian with 13 years of combined Information Assurance/Cyber Security engineering and defensive/offensive cyberspace operations research and development experience. He holds both a bachelor's and master's degree in Computer Science from Polytechnic University. Mr. Raio maintains several professional certifications including Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC) Certified Unix Security Administrator (GCUX), and GIAC Certified Forensic Analyst (GCFA). Mr. Raio is also an Army acquisition professional certified level 3 in Systems Planning, Research, Development and Engineering (SPRDE) Systems Engineer career field and a member of the Army Acquisition Corps. In addition to his professional accomplishments, Mr. Raio plays an active role in community outreach efforts promoting Science, Technology, Engineering and Mathematics (STEM) education among students.

Cyber Security and Information Systems
Information Analysis Center
266 Genesee Street
Utica, NY 13502



THE CENTER OF EXCELLENCE IN CYBER SECURITY AND INFORMATION SYSTEMS

Leveraging the best practices and expertise from government, industry, and academia in order to solve your scientific and technical problems

https://www.csiac.org/journal/