Hardening Mission Operations Against Cyber Threats

J. Weaver, L. Wihl
SCALABLE Network Technologies
Culver City, CA
jweaver@scalable-networks.com
lwihl@scalable-networks.com

ABSTRACT

In the multi-domain battlefield, our warfighters rely on a geographically dispersed, connected network of sensors, platforms, and weapon systems to prosecute their missions in harsh and contested environments that complicate the detection of compromised communications. Mission rehearsal must accurately incorporate the evaluation of cyber resilience of missions in a holistic survivability context based upon realistic tactical environments that reflect intrinsic cyber weaknesses. These evaluations must understand how the adversary will deploy cyber threats during multi-domain operations and the associated impacts of the adversary's mission-specific tactics, techniques, and procedures.

Traditional cyber ranges are used to assess cyber vulnerabilities but are challenged with the accurate representation of missions and systems, and associated impacts due to adversary actions. It is important to note that every cyber vulnerability is not necessarily a mission or system vulnerability, because the cyber vulnerability may or may not impact the system capability needed to successfully complete the mission. From a mission perspective, cyber security is not a computer problem, but is rather a weapon system engineering problem. Weapon systems must be assessed differently from enterprise networks and general cybersecurity expertise is not the same as weapon system cybersecurity expertise.

In this paper we present an new approach aimed at desktop analysis of mission scenarios, the mission-centric cyber range, that addresses these limitations through integration of cyber and kinetic domains. This approach integrates IP and non-IP communications (e.g., 1553 bus) and represents wireless and tactical waveforms with their specific vulnerabilities. We use an extensible attack library to exploit vulnerabilities in networks, connected weapons, and C2 subsystems. Finally, we assess in parallel the command staff's ability to execute multi-domain operations and network defenders to detect and react to threats within a contested environment. Utilizing this approach, the authors present findings for an undersea warfare mission regarding the adequacy of defenses against cyber-attacks that attempt disruption of situational awareness.

ABOUT THE AUTHORS

Dr. Jeffrey Weaver is Vice-President of Engineering at SCALABLE. He obtained his Ph.D. degree in Electrical Engineering as an NSERC-PGS Scholar from Western University in Ontario, Canada. Dr. Weaver has held key technical and executive engineering roles during his career and has over 25 years of product development experience in hardware and software systems. His research interests include digital communication and propagation modeling using switched stochastic differential equations, signal processing and hybrid analytical-numerical modeling techniques. Dr. Weaver has seven patents in the areas of IP routing, VLAN, QoS, and high-performance hardware design.

Lloyd Wihl is Director of Application Engineering at SCALABLE Network Technologies. He has 30+ years' experience in the Modeling, Simulation and Training industry, developing system architectures and leading multi-million-dollar projects in the areas of synthetic degraded digitized battlefields, distributed mission operations, network-centric systems, air combat, marine systems, space systems, visual systems, and flight simulation. He is a recipient of the NASA achievement award, has published and presented several papers on synthetic environments, and guided development of SCALABLE's live-virtual-constructive cyber training system that integrates cyber and kinetic warfare.

Hardening Mission Operations Against Cyber Threats

J. Weaver, L. Wihl
SCALABLE Network Technologies
Culver City, CA
jweaver@scalable-networks.com
lwihl@scalable-networks.com

PROBLEM

Complex supply chains are an important part of modern weapons manufacturing. The risk of unintended interactions among systems is increased when systems are continually expanded and revised. While the risk of malicious actors attempting unauthorized access to computing systems is substantial and growing, the role and risks associated with malicious insiders must be considered since unauthorized actions within one administrative domain can lead to subsequential unauthorized effects in other federated IT systems.

The market has responded with an evolution of intrusion detection systems (IDS), intrusion protection systems (IPS), firewalls, managed detection services (MDS), and other similar capabilities, each intended to address a complementary market. This array of technology aims to create a web of overlapping capabilities to protect IT systems. This web, though, itself might have gaps and not fully evaluate interactions with other systems. It is left to each IT organization itself to decide what is "enough".

Modern IT organizations – in both defense and commercial contexts – follow directions provided by a number of well-known and evaluated strategies such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of service (STRIDE) (Hernan, Lambert, Ostwald, & Shostack, 2006) and risk-to-mission assessment process (RiskMAP) (Watters, Morrissey, Bodeau, & Powers, 2009). These strategies assist the IT designer of a target architecture to identify shortcomings and create conditional attack chains which help regularize the design patterns used in the network to limit information losses by increasing surveillance or requiring multiple obstacles to access critical information. These information losses can be evaluated to identify the risk of loss using informal analysis or a more formal loss evaluation methodology such as the NIST Risk Management Framework (RMF) (National Institute of Science of Technology, 2021).

Ultimately the link between architecture, technology, and risk evaluation is a manual process. Mitigating unlikely risks costs extra resources and can lead to additional operations fragility. In a military context, the focus is either on the "most dangerous" or "most likely" risks. A tool to support both approaches must accurately score and assign probability to outcomes. Accurately assessing these risks during planning or review reduces the likelihood of unknown and unbounded risks whether measured in dollars or, in the military context, lives and national security. Cyber incursions increase year over year in both volume and capability. (Miller, 2020) Cyber warfare is an established doctrine of our adversaries (Colarik & Janczewski, 2012). Within the DoD there is an underserved need to assess systems-of-systems cyber resilience from multiple, diverse, dynamic, and adaptive adversaries that exploit communications networks as attack surfaces. This leads to the core question: how do we connect architectures, technologies and risk and analyze our systems in the emergent cyber domain?

Cyber security is not only a computer problem but also an engineering problem (Barnett, 2020). In the particular domain of weapons systems engineering, it provides an opportunity to respond to the emerging cyber warfare activities. Retaining, and mitigating the risks to, system capability must be the focus of a workflow. This workflow begins with an architecture, is implemented using technologies available and is analyzed to provide input into risk management activities. This analysis capability must provide methods to assess dynamic, emergent resilience at a system of systems level, in this case for analyzing potential end-to-end impacts from implementing Joint All Domain Command and Control (JADC2) concepts and systems. JADC2 is the US military's concept to connect sensors from all military branches into a single shared network. For this experiment, we use the EXata™ simulator from Scalable Network Technologies to evaluate candidate architectures that incorporate cyber hardening

techniques for self-healing networks. We evaluate a mission longitudinally over its evolution and quantify how design changes affect mission success.

The systems that comprise JADC2 operate on a geographically dispersed, connected network of sensors, platforms, and weapon systems operating in harsh and contested environments to achieve mission success. In this era of renewed strategic competition and sophisticated cyber threats, it is imperative that we assess the cyber resilience and survivability of networks in the context of the missions they support. Such an assessment should be based on mission objectives, weapon system attributes and vulnerabilities, network defense capabilities and adversary techniques, tactics and procedures.

Every cyber vulnerability in a weapon system or underlying network is not necessarily a mission vulnerability because exploitation of the cyber vulnerability by the adversary may or may not impact the ability to successfully complete the mission. To appropriately assess mission cyber resilience, it is necessary to assess the weapon or network cyber resilience in a realistic tactical environment. Thus, to ensure cyber resilience throughout the JADC2 environment, and hence mission success, military commanders need a capability to predict the impact and frequency of potential cyber-attacks on a specific mission and analyze alternative mitigation strategies within the context of the mission.

In the following sections we discuss the evaluation approach and proposed methodology, identify its benefits and provide an instructive example of those benefits when applied to a specific use case.

APPROACH

Network Digital Twin technology applies digital engineering techniques to cyber analysis. This allows the use of digital engineering techniques to be applied to the mission level with visibility in all network activities and protocols encountered in routine and anomalous situations. System of systems network digital twins are necessarily multi-domain system, consisting of cyber, air, surface, space and undersea activities. One area of significant interest in the industry today is 5G cellular. More than previous approaches (e.g., 4G/LTE), 5G has an open architecture within the core (i.e., Open5GCore) which creates both radio- and protocol-level interactions but also significant IT infrastructure exposure.

Furthermore, commercial business, critical infrastructure and defense missions rely on the broad interconnection of systems to succeed. True digital engineering relies on integrated digital representations to be available for supervisory control and data acquisition (SCADA) systems, MIL-STD 1553 busses and serial line devices. Disruptions in network operations due to kinetic and non-kinetic weapons are additionally required for defense scenarios due to the specialized military environment. It cannot be emphasized strongly enough that non-kinetic cyber warfare is increasingly being directly waged on the civilian population by government and non-government actors requiring the same digital engineering activities to be used by private enterprises, such as banks, that previously could operate in relatively security.

The military operates many custom radio networks each designed with different measures to avoid detection, interference and geolocation. It is critical to reflect those capabilities in a cyber scenario since they directly have an impact on the success of the military mission. Additionally, the propagation effects must account for data-driven losses such as those due to terrain and manmade structures. Without “closing the loop” from the local device area networks (e.g., 1553 bus) to tactical wireless to reach-back to command facilities –and furthermore incorporating the live applications that rely on that system -- it is difficult to assess the efficacy of the proposed mission architecture or the risk of mission failure.

In this area, traditional commercial cyber ranges might in turn both over- and under-deliver. They are designed to replicate, with high fidelity, a specific experiment or environment particularly at the IT-level. It rarely makes sense, though, to create a scenario – or tens or hundreds of scenarios – to analyze potential outcomes within such an environment. The ability to create a software integration environment is important to identify and evaluate “unknown unknowns” but lack the flexibility to perform mission analysis. The amount of reconfiguration required to reflect a hypothetical intrusion or defense reflects the complexity of the system itself. This is analogous to using an IT laboratory to forecast IT costs. While it is possible to assign a cost to each piece of equipment and calculate it manually, it is simply much easier to use a spreadsheet tool such as Excel™ to sum costs in a straightforward

manner without setting up the laboratory. Digital engineering is complementary to cyber range systems and results from each tool informs each other and the state of best practices for information systems.

Large cyber ranges can incorporate both wired and wireless system components. Wireless has had an important role in the defense sector and many modern commercial capabilities reflect earlier military use. As discussed, electronic warfare must consider whether a signal should be emitted at all, where it might be received and whether the adversary has enough territorial control and equipment to identify the location of the transmitter. Likewise, as in all test situations, some level of kinetic and non-kinetic integration must be achieved to identify changes to mission risk as the environment becomes contested and degraded. Tools to support example environments such as that exemplified by the I/ITSEC Operational Blended Warrior (OBW) (Moore, Chaney, & Flint, 2018) including COATS (Wells & Bryan, 2015), CORONA (Norman & David, 2013) and StealthNet (Torres, et al., 2015) and each have proven value to defense. In this paper, we build upon these capabilities to provide an easy-to-use cyber resilience evaluation tool suitable for deployment to planners and operators alike. LVC remains an important activity for testing but is less valuable for analysts and designers who need planning applications to perform what-if analysis based on proposed architectures as part of the experiment planning process.

This is the capability gap that is filled by the network digital twin capability that develop a digital engineering level mission clone. This clone provides advanced training and assessment solutions to assess and improve cyber resilience of missions that comprise the JADC2 umbrella

For purposes of this paper, a network digital twin refers to a computer simulation model of the communication network together with its operating environment and the application traffic carried by it. It can be used to study the behavior of its physical counterpart in a low-cost and zero-risk environment, either in theater or in the laboratory. To do so effectively, the digital twin must have sufficient fidelity to accurately reflect the network dynamics due to the interplay between the communication protocol, device configurations, network topology, application traffic, the physical environment, and the cyber-attack. For instance, the location, intensity, and duration of a jamming or denial of service attack launched by an adversary, will determine their impact on communications that are critical to the mission. The interference needed to disrupt streaming video, may be very different from that needed to disrupt Positioning, Navigation and Timing (PNT). And the digital twin must have sufficient fidelity to capture the network dynamics and thus appropriately discriminate among cyber-attacks that are a mere annoyance from those that have the potential to disrupt the mission timeline.

This approach has substantial benefits. The first and foremost is the ability to perform detailed analysis across all communications and networking domains. This allows system-level metrics to be derived from the large amount of technical data that is generated during modern simulation. This integration includes direct integration with the cyber-physical domain and simulation systems such as the HyperSim-EXata from SCALABLE and OPAL-RT (OPAL-RT, 2019). Using this end-to-end approach, a wide variety of cyber-attacks can be launched against networked reconnaissance, C2 systems and connected munitions. Moreover, due to the more limited goals of a mission clone it is possible to shrink the processing footprint of the software so that it can be deployed on cloud or local COTS computing hardware.

Portraying and analyzing the effects of threats in high fidelity is important to two use cases. The techniques described in this paper are useful to command and staff to thoroughly analyze hypothetical operations and doctrinal IT changes that affect the risk to mission success. The rapid turn-around time to evaluate changes allows its use even during live events. It is also useful for network defenders to rapidly detect and react to cyber-threats as they unfold. As indications of threats emerge, a mission clone updates its threat environment (and metrics) and allows the network defenders to evaluate specific strategies to neutralize the threat.

Our mission clone consists of the following primary components: mission network model, real-time interfaces, and a model library. These include cyber, network and communication models configured from multiple sources (Visio™ diagrams, live network scans, and any other available source data). The wireless models include SATCOM, 5G, LTE, Wi-Fi and sensor networks, and tactical models include WNW, SRW, MUOS, EPLRS, SINCGARS, WIN-T (NCW, HNW), BFT, IFF Mode 5, ANW2, TTNT, and CDL.

A suite of simulated cyberspace attacks and defenses can interact with every layer of the emulated network. These include network security protocols, firewall models, port and network scanning, eavesdropping, jamming and silent jamming, denial of service, packet modification, wormholes, signals intelligence, stimulation of intrusion detection systems, phishing, vulnerability exploitation, virus and worm propagation and defense, backdoors, rootkits, botnets,

and others. Host models can be configured with memory, CPU cycles, vulnerabilities, processes, and shared files which can get infected.

This tied together with a cyber mission specification capability supports development of distributed and adaptive cyber missions and interface with the underlying kinetic operations. This mission editor enables the user to graphically create cyber-attacks, their timing and logic, and how they will progress depending on actions taken during the mission. The resultant attack script will execute in conjunction with the mission network models using feedback from device states and user actions.

Human operators participate in the exercise at friendly or adversary stations, using their own repertoire of real discovery, attack, monitoring, and defense tools. Adversary players can use real malware and exploitations, as well as launch simulated attacks, to attack the network digital twin and the connected components. The operators try to accomplish their mission while monitoring and defending the network using their actual tools. The approach allows operators to learn individually and as teams to detect when something is wrong, assess what is happening, contain the attack, take countermeasures, and modify operations to assure the mission. It also enables command and staff to work around the cyberspace operations and complete a mission, while network administrators learn to detect and react to threats as they occur, in the same exercise. An after-action review capability plays back any operators' screenshots and all their actions (clicks, keystrokes, chat messages and voice calls) on a moving timeline along with attacks and their progression, other operators' views, and the actual state of the network and mission.

IMPACT OF APPROACH

The mission clone extends the approach to cyber resilience past the concept of experiments and tests. This allows mission network analysts to directly propose an architecture based on industry and military best practices, such as MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) (The MITRE Corporation, 2021) evaluate the mission against metrics and key performance parameters (KPP) and use them to determine mission risk. These results can be analyzed and integrated back into the baseline architecture and analyze differences between plan revisions culminating ultimately with actual performance in the field.

The mission clone provides the mission network designer with a new avenue of semi-automated mission network analysis that directly integrates with several sources of information, software systems and directly informs risk analysis. This analysis can be done on the desktop, the laptop or the cloud.

EXAMPLE USAGE AND RESULTS

With a mission-centric cyber range, we are now able to better represent a mission subject to cyber-attack. The mission centric cyber range provides network behavior, connectivity, and weapon system susceptibility to cyber-attacks, to help assess cyber threats in the context of the mission. We built a prototype testbed using the Navy's Next Generation Threat System (NGTS), EXata, and live applications in the loop, to investigate the effect of malware injection and deception operations on blue force command and control.

The environments in which multi-domain tactical communications operate can make it hard to distinguish between electronic warfare/cyber-attacks and signal losses from effects such as interference and noise. As an example, undersea communication networks are particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. Attackers could capitalize on these characteristics to produce connections via low latency radios (above the water surface) that act as wormholes, enabling man-in-the-middle attacks that can totally drop ("black hole"), selectively drop ("gray hole"), or modify messages. The problem is exacerbated with the incorporation of unmanned vehicles; the resulting dynamic topology of a mobile, low bandwidth undersea detector network facilitates the launching of man-in-the-middle attacks and complicates their detection.

We developed an experiment simulating an undersea warfare (USW) mission, integrating platform positions and mobility, a simulated USW tactical network, simulated cyber-attacks, networked system performance, external interfaces for live data, and the influence of cyber-attacks on the operating picture. The USW tactical network is shown in **Figure 1**.

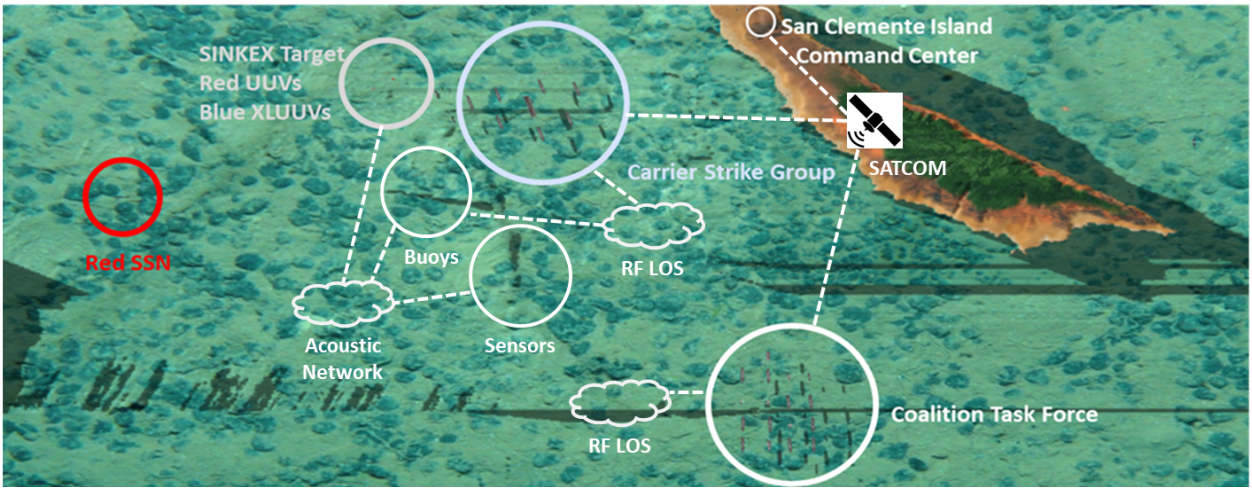

Figure 1: USW tactical network

We created a scenario with two large groups of surface ships. The coalition task force is modeled on the Rim of the Pacific Exercise (RIMPAC) coalition task force that had about 24 ships participating in 2020. One of the events was a sink at-sea live-fire training exercise (SINKEX) of a decommissioned US amphibious cargo ship. We modeled the conclusion of the SINKEX when the coalition force is heading back out to sea. They also participate in a passing exercise with the carrier strike group that is deploying and is headed to the western Pacific. In addition to the surface activities, there is undersea activity: two blue extra-large unmanned undersea vehicles (XLUUVs) are searching for and conducting surveys of that SINKEX target, and they will transmit some video back to the command center ashore.

In our experiment, one of the destroyers (DDGs) in the coalition task force from South Korea was attacked with malware from North Korea and it is unwittingly inserting that malware into the network via communication links. Unbeknownst to the blue side at the start of the scenario, there is also a red attack submarine (SSN) and two red unmanned undersea vehicles (UUVs). The SSN has been monitoring the SINKEX and launched a couple of UUVs to try to gather some intelligence from the results of the SINKEX. In the scenario there are also undersea sensors that will come into play as they detect the red submarine. There are also two MH-60R helicopters flying with the carrier strike group and they will be participating in the exercise when the red submarine assets are detected.

Figure 2 shows the visualization of the coalition force and the carrier strike group using SCALABLE's Scenario Player. The vessels' locations are continually updated, and lines dynamically animate communication links, showing message routing and achieved data rates.

Figure 2: Visualization of coalition forces

There are several undersea sensors sitting on the seabed. There are multiple sonobuoys to the north and south of the carrier strike group. A couple of helicopters fly over the coalition force, capturing video and streaming it back to the command center. The carrier strike group is accumulating data from the undersea sensors as well as the sonobuoys, assembling the operational picture.

There are a couple of undetected red UUVs. One of them approaches the sunken ship to observe it. The other red UUV will inject some cyber-attacks which are going to disrupt the operational picture and give the command center an incorrect view of the undersea environment.

One of the undersea sensors picks up an acoustic signal from the red submarine and is relaying that up to a sonobuoy which is then sending the detection signals over to the carrier strike group. From there, all the sensor data is being amalgamated and sent over to the command center. The command center captures and displays the data coming in from both the carrier strike group and the coalition force. On three of the screens, we see live video from the XLUUV at the sunken ship, and the two helicopters flying over the coalition force. The actual video streams are run through our network emulation and are subject to disruption by cyber-attack.

The results we obtained are as follows. Initially, all the computers are secure. However, as the scenario progresses, the South Korean DDG begins to communicate to the command center. The DDG had been infected with malware from North Korea. The malware now propagates over the network to the command center. As it spreads through the command center network, it infects additional computers, which freeze, as visualized by red symbols (**Figure 3**).

Figure 3: Simulated command center

The video from one of the helicopters has been interrupted by the malware which is disrupting the flow of communication. The other helicopter's video still gets through.

The operational picture shows the positions of the ships and the red SSN which was detected by the undersea sensor. Initially, the picture is correct (**Figure 4)**. However, one of the red UUVs launched another attack. It is emitting an incorrect signature which is picked up by the sensors and interpreted to be a second red submarine (Figure 5).

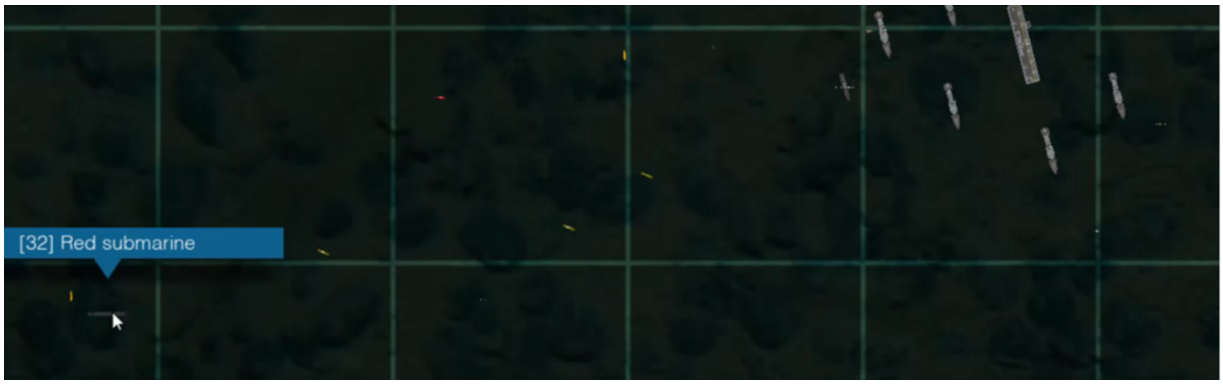

Figure 4: Initial operating picture

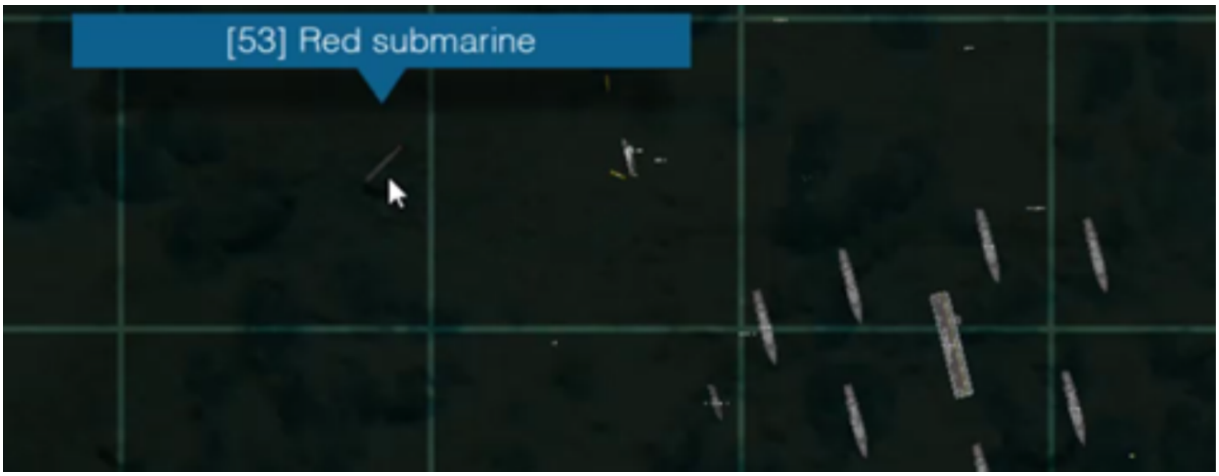

Figure 5: Disrupted operating picture

The two MH-60R's are deployed: one to where the red submarine is, and the other is deployed incorrectly to the fake position which is spoofed by the red UUV.

Our key findings were that we could model a system of systems with vulnerabilities related to a distributed network of sensors, platforms, communications, and C2. As simulated cyber-attacks were injected, not every attack turned out to be of equal importance in the mission context. The helicopter imagery disruption was merely an annoyance, with minimal impact on the mission. We also noted that traditional IT defenses were only partly applicable; they would not have protected from the spoofing that rendered the operational picture wrong. The cyber-attacks were able to affect the mission, causing the MH-60R to move to the wrong position. In the context of the mission, being able to correctly identify systems that have become compromised and untrustworthy may turn out to be more important than striving to defend all individual systems.

CONCLUSION

Mission analysis – whether it be conducting business smoothly, keeping our critical infrastructure safe, or conducting successful defense operations – continues to be an important, multi-disciplinary activity. Cyber-enabled analysis is more important than ever and will continue to dominate networked system architecture development for the foreseeable future. In this paper, we identified the main impediment to end-to-end cyber analysis is the lack of an environment to rapidly evaluate the effects of an attack on a candidate network and provides quantitative data that can be used as input to other risk management processes.

Based on this vision, we intend to continue to expand the role of digital engineering and the mission clone. In particular, we see an unmet need to incorporate Model Based System Engineering (MBSE) tools into the risk reduction workflow. There is also a high-level need to expand the library of cyber defense technologies and procedures available in our cyber thread editor. Finally, when we interface with high-level tools it is critical to map system elements one-for-one into the simulation context. In any event, the evolution away from isolated network analysis toward a holistic mission view will continue to occur using our tools and others filling a similar need.

ACKNOWLEDGEMENTS

Authors acknowledge this work was partially supported under NAVSEA contract #N6833520C0824 (Digital Theater-level System Model for Cyber Security Analysis).

REFERENCES

Barnett, T. (2020). A Mission-Based Cyber Approach. *JNE Users Group Presentations.* Culver City, CA: Scalable Network Technologies.

Bodeau, D., Graubart, R., McQuaid, R., & Woodill, J. (2018). *MTR180314: Cyber Resilience Metrics, Measures of Effectiveness, and Scoring.* The MITRE Corporation.

Colarik, A., & Janczewski, L. (2012, Spring). Establishing a Cyber Warfare Doctrine. *Journal of Strategic Security, 5*(1), 31-48.

Duong, H., Salisbury, B., Bagrodia, R., & Dietz, S. (2018). Assessing Cyber Resilience of Military Systems using LVC Models. *Proceedings of I/ITSEC 2018.* Orlando, FL: I/ITSEC.

Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. (2006, Nov). Uncover Security Design Flaws using the STRIDE Approach. *MSDN Magazine*.

Ixia Communications. (n.d.). *Cyber Range: Improving Network Defense and Security Readiness.* Retrieved Feb 2021, from Ixia Communications: https://support.ixiacom.com/sites/default/files/resources/whitepaper/915-6729-01-cyber-range.pdf

ManTech International Corporation. (n.d.). *Advanced Testing, Evaluation and Cyber Training.* Retrieved Feb 2021, from ManTech International: https://acre.mantech.com

Miller, M. (2020, Apr 16). *FBI sees spike in cyber crime reports during coronavirus pandemic*. Retrieved from The Hill: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

Moore, S., Chaney, M., & Flint, L. (2018). Cyber Experimentation through Operation Blended Warrier. *Proceedings of I/ITSEC.* Orlando, FL: I/ITSEC.

National Institute of Science of Technology. (2021, May). *NIST Risk Management Framework*. Retrieved from Computer Security Resource Center: https://csrc.nist.gov/Projects/risk-management/about-rmf

Norman, R., & David, C. (2013, Summer). Cyber Operational Research and Network Analysis (CORONA) Enabled Rapidly Reconfigurable Cyberspace Test and Experimentation. *M&S Journal*, pp. 15-24.

OPAL-RT. (2019, Oct 17). *Product News*. Retrieved from OPAL-RT: https://www.opal-rt.com/opal-rts-hypersim-scalables-exata-cps-real-time-cyber-physical-simulation-of-the-electric-power-grid-for-cybersecurity-studies/

Palo Alto Networks. (2021, Apr 29). *Cyber Range.* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/cyber-range

The MITRE Corporation. (2021). *MITRE ATT&CK (v9)*. Retrieved from https://attack.mitre.org

Torres, G., Smith, K., Buscemi, J., Doshi, S., Duong, H., Xu, D., & Pickett, H. K. (2015). Distributed StealthNet (D-SN): Creating a live, virtual, constructive (LVC) environment for simulating cyer-attacks for test and evalution (T&E). *Proceedings of MILCOM 2015.* Tampa, FL: IEEE.

Watters, J., Morrissey, S., Bodeau, D., & Powers, S. (2009). *The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues.* The MITRE Corporation.

Wells, D., & Bryan, D. (2015). Cyber Operational Architecture Training Systems - Cyber for All. *Proceedings of I/ITSEC 2015.* Orlando, FL: I/ITSEC.

Wihl, L., Varshney, M., & Kong, J. (2010). Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments". *Proceedings of I/ITSEC 2010.* Orlando, FL: I/ITSEC.