Enhancing Cyberweapon Effectiveness Methodology with SE Modeling Techniques: Both for Offense and Defense

C. Ariel Pinto
Old Dominion University

Matthew Zurasky
Old Dominion University

Fatine Elakramine

Safae El Amrani

Raed M. Jaradat

See next page for additional authors

Original Publication Citation

Pinto, C. A., Zurasky, M., Elakramine, F., Amrani, S. E., Jaradat, R., M., Kerr, C., & Dayarathna, V., L. (2021). Enhancing cyberweapon effectiveness methodology with SE modeling techniques: Both for offense and defense. *International Journal of Cyber Warfare and Terrorism 11*(3), 41-57. https://doi.org/10.4018/IJCWT.2021070104

Enhancing Cyberweapon Effectiveness Methodology With SE Modeling Techniques:

Both for Offense and Defense

C. Ariel Pinto, Old Dominion University, USA

Matthew Zurasky, Old Dominion University, USA

Fatine Elakramine, Mississippi State University, USA

Safae El Amrani, Mississippi State University, USA

Raed M. Jaradat, Mississippi State University, USA

Chad Kerr, Mississippi State University, USA

https://orcid.org/0000-0001-7583-6863

Vidanelage L. Dayarathna, Mississippi State University, USA

https://orcid.org/0000-0002-6119-0261

ABSTRACT

A recent cyberweapons effectiveness methodology clearly provides a parallel but distinct process from that of kinetic weapons – both for defense and offense purposes. This methodology promotes consistency and improves cyberweapon system evaluation accuracy – for both offensive and defensive postures. However, integrating this cyberweapons effectiveness methodology into the design phase and operations phase of weapons systems development is still a challenge. The paper explores several systems engineering modeling techniques (e.g., SysML) and how they can be leveraged towards an enhanced effectiveness methodology. It highlights how failure mode analyses (e.g., FMEA) can facilitate cyber damage determination and target assessment, how block and parametric diagraming techniques can facilitate characterizing cyberweapons and eventually assess the effectiveness of such weapons and conversely assess vulnerabilities of systems to certain types of cyberweapons.

KEYWORDS

Cyberweapons Effectiveness, Model-Based Systems Engineering (MBSE), Offense and Defense, Security Modeling Language (SecML), System Modeling Language (SysML)

INTRODUCTION

Cybersecurity is now ubiquitous both in the civilian and the military arena. In the military arena, cyber warfare has several advantages over conventional warfare. First, there are fewer human lives at stake during mission execution because it does not necessarily require “boots on the ground”

DOI: 10.4018/IJCWT.2021070104

or kinetic munitions during deployment. Second, the actual deployment can be initiated without limitations such as weather, visibility, and spatial proximity, which all presents limits for kinetic weapons. Lastly, cyberweapons can be cheaper than traditional munitions attacks as cyberweapons development requires different sets of infrastructure and resources from kinetic weapon development, as well as its replicability and reusability. As cyberweapons become more common, technologies in the cyber warfare domain would require more information sharing among the various stakeholders. Cyberweapons effectiveness analysis is emerging not only for an offensive purpose (i.e., to attack a target) but also for a defensive purpose (i.e., to defend assets from cyberweapons).

In systems development, there are many "-ilities" that are designed into the system from the start – such as reliability, maintainability, sustainability, usability, and so on are qualitative design requirements that must be met. The complexity and rapidly evolving technologies in the cyber warfare domain pose a challenge for engineers to improve cyber weapons development, including requirements analysis and eventual deployment. In this paper, we propose the use of systems engineering modeling domain, such as using tools like Systems Modeling Language (SysML) and how they can be used in cyberweapon effectiveness prediction methodology. The cyberweapons domain would greatly benefit from similar approaches and may eventually lead to a model-based systems engineering (MBSE) approach to cybersecurity, offense-informed and defensive-informed design scenarios.

Today's systems engineers use Model-Based Systems Engineering (MBSE) through tools and languages, like SysML, to capture requirements, use cases, system hierarchies, functions, and interfaces. SysML provides a central point of information used by system designers and users to evaluate and analyze system development and performance. Cybersecurity, as with the other "-ilities," can be included in the SysML modeling using Security Modeling Language (SecML), which utilizes features from SysML to modeling security-specific system needs.

This paper presents an enhancement to a cyberweapons effectiveness methodology developed by Pinto and Zurasky (2020) by adapting various SysML techniques to better promote consistency and improve cyberweapon system evaluation accuracy for both offensive and defensive postures. The paper includes examination and potential adaptation of systems engineering modeling technique (i.e., SysML) into the design and operations phases of cyberweapon systems development and how these same attempts can be leveraged to enhance prediction processes during cyber offense and defense. This paper will review the previously developed cyberweapons effectiveness methodology, examine the integration of systems modeling (i.e., SysML) into this methodology, and finally, show how these can be leveraged to enhance prediction methodology during cyber offense and defense via a case study.

BACKGROUND

With the current increase in technology, the world is shifting towards digitization, making it more vulnerable to cyber-attacks. This continuous shift in various dimensions of risk – including those in the cyber realm – is characteristic of the complex nature of risk itself (Pinto et al. 2012). These cyber-attacks are proven to be of great damage to companies, customers, and nations, which makes cybersecurity a necessity (DiMase et al., 2015). Cybersecurity has become one of the most important topics globally, as countries worldwide provided their stance on cybersecurity (Klimburg, 2012; Tatar, Ü, et al., 2014). Systems engineering methodologies can be acquired to enhance cybersecurity for addressing cybersecurity issues. For example, Bayuk et al. (2011) highlighted beneficial systems engineering strategies that can solve frequent system security problems. In their work, Bayuk et al. (2011) focused on the benefits systems engineers can provide to the cybersecurity issue. In this paper, we merge two methodologies, a cyberweapons assessment methodology and a systems engineering methodology, to show the utility of using systems engineering in the domain of cyberweapon assessment.

CYBERWEAPONS ASSESSMENT METHODOLOGY

Pinto and Zurasky (2020) recently described an effectiveness assessment and prediction modeling for cyberweapons as an enhancement to the domain of kinetic weapons. It described how the standardization of the formulation and methodology provided a common framework including processes, definitions, and assumptions to consistently perform assessments for both cyber and kinetic weapons. That contains four primary phases, as shown in Figure 1. These phases are: Cyber damage determination, Cyberthreat assessment, Cyberweapon characterization, and Cyber effectiveness estimate generation.

The first phase of the methodology is related to the prediction of the possible damage that might impact the cyberweapons. Cyber-specific damage effects may include those listed in Table 1, as described in Zurasky (2017) and Pinto and Zurasky (2020). The effects are described along with important metrics such as how long it takes to execute the effect (latency) and how long it continues to execute the effect (persistence). The damage effects can have wide variations in the outcome, from simple unavailability to a more severe data modification, i.e., altered in a manner that is intended to appear genuine to the user to affect downstream processes and procedures. All these may eventually lead to disruption of downstream operation and could lead to physical damage. In 2017 a security company called Naval Dome showed just how vulnerable ships were to cyberweapons. The company demonstrated the ability to alter the ship's position (heading and speed) and modify radar displays without drawing suspicion (TME, 2017).

Figure 1. Cyber effectiveness methodology (adapted from Pinto & Zurasky, 2020)

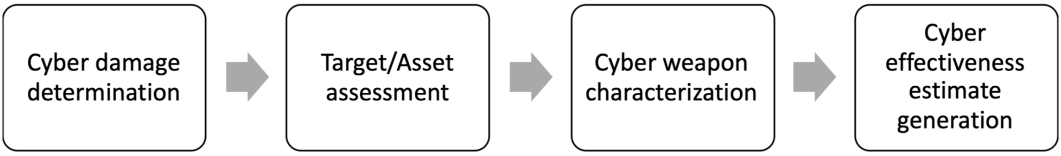

Cyber damage determination
Target/Asset assessment
Cyber weapon characterization
Cyber effectiveness estimate generation

Table 1. Cyber effects, brief description, and sample metrification (adapted from Zurasky, 2017)

Cyber damage	Brief Description	Sample Metrics
Unavailability of network resources	Network resources made unavailable to intended users by temporarily or indefinitely disrupting services of a host connected to the Internet (e.g., a similar effect to Distributed Denial of Service (DDoS) attack)	Latency: immediate Persistence: 5 minutes (DoS), four hours (DoS4), or 24 hours (DoS24)
Misinformation	False or incorrect information is spread intentionally to affect down-stream processes and procedures	Latency: gradual Persistence: 5 minutes (MisI), four hours (MisI4), or 24 hours (MisI24)
Data Modification	Data is inserted, deleted, or altered in a manner that is intended to appear genuine to the user to affect down-stream processes and procedures	Latency: immediate to gradual Persistence: 5 minutes (DMod), four hours (DMod 4), or 24 hours (DMod 24)
Data Repudiation	Data or information is made to appear to be invalid or misleading to affect down-stream processes and procedures	Latency: immediate Persistence: 5 minutes (DRep), four hours (DRep 4), or 24 hours (DRep 24)
Spoofing	Masquerade as someone else	Latency: immediate Persistence: indeterminate

In the second phase – target/asset assessment, the target to be attacked or asset to be defended must be accessed from a cyber perspective. This phase was partly patterned on assessment methods typically used for kinetic weapons, which includes threat identification, modeling, and vulnerability assessment. During this phase, information about the target/asset is collected with all the relevant information required for analysis. Modeling the target/asset includes details of the various operations, networking, failure modes, reliability, and potential vulnerabilities. Finally, the vulnerabilities found through analysis and modeling can be assessed for the critical cyber components. Samples of previously exploited vulnerabilities are listed in Table 2.

The third phase, cyberweapons characterization, is where metrics for cyberweapons are developed to align with the mission or use case for the cyberweapon system. For example, a reconnaissance mission includes network mapping and search algorithms to identify paths to infiltrate the target/asset system. Lateral movement missions include moving within the network along the best path to the target/asset system. This is accomplished by infiltrating neighboring and trusted networks and incrementally gaining higher-level authorities to access the target/asset. Lastly, a payload deployment mission executes the malicious code to exploit the vulnerabilities of the target/asset system. Full characterization and mission assessment of the cyberweapons provides critical insight into the processes employed to gain entry. These paths or flows of the weapon provide additional points where mitigations can be implemented into the system design. The sequential missions of the cyberweapon are the equivalent "kill chain" of the kinetic weapon world. Lockheed Martin (Lockheed Martin, 2020) develop the Cyber Kill Chain framework that follows a similar path of 1) Reconnaissance, 2) Weaponization, 3) Delivery, 4) Exploitation, 5) Installation, 6) Command and Control, and 7) Actions

Table 2. Cases of exploited vulnerabilities (adapted from Sood and Enbody, 2014)

Vulnerability Types	Description	Vulnerable Systems Examples
Backdoors and Hardcoded Passwords	Hardcoded passwords embedded in the firmware that allow attackers to gain complete access	Supervisory Control and Data Acquisition Systems (SCADA) provided by Siemens, TURCK, etc. were vulnerable (TURCK CVE, 2012)
Insecure Authentication and File Uploading	Security issues arising from the inability of the systems to implement granular control through proper authentication and authorization checks	Global Positioning System (GPS) Satellite Communication (SATCOM) systems provided by Harris, Cobham, JRC, Iridium, and Hughes were vulnerable (Warner et al., 2012)
Remote Code Execution	Security issues such as buffer overflows, memory corruption, privilege escalations, dangling pointers in operating system components, browsers, critical systems such as ICS/SCADA, routers, other software such as Microsoft Office, Adobe Reader, Java, etc.	SCADA systems provided by ICONICS GENESIS32, BizViz, IntegraXor, Sielco Sistemi, etc. were vulnerable to Buffer Overflows (InfoSec, 2011) XMLDOM Zero-day vulnerability was exploited to attack the U.S. Veterans of Foreign Wars' website (Gonsalves, 2014) Operation Pawn Storm uses vulnerabilities in M.S. office files to target U.S. military officials (Paganini, 2014)
SQL Injections	Weaknesses in web applications that allow attackers' queries to be executed directly in the backend database	Royal Navy website hacked using SQL Injection (BBC News, 2010) U.S. Army website hacked using SQL Injection (Dark Reading, 2010)
Insecure Protocols, Spoofing, and Hijacking	Undocumented and insecure protocols allow hijacking and spoofing of communication channels	Common Channel Signaling System 7 (CCSS7) in the U.S. or Common Channel Interoffice Signaling 7 (CCIS7) in the U.K., (The Guardian, 2016) Possible attacks to spoof GPS communication to control U.S. drones (Schwartz, 2011)

on Objectives. With the proper characterization of the mission and kill chain of the cyberweapon, each step in the chain can be assessed for mitigation steps to reduce the susceptibility of the system to an intrusion.

The final phase – cyber effectiveness estimate generation, quantifies the impact of exploiting the vulnerability in the target/asset system, designated as Probability of Cyber Kill (P_{ck}). Pinto and Zurasky (2020) developed the cyber equivalent probability of kill P_{ck} equation as:

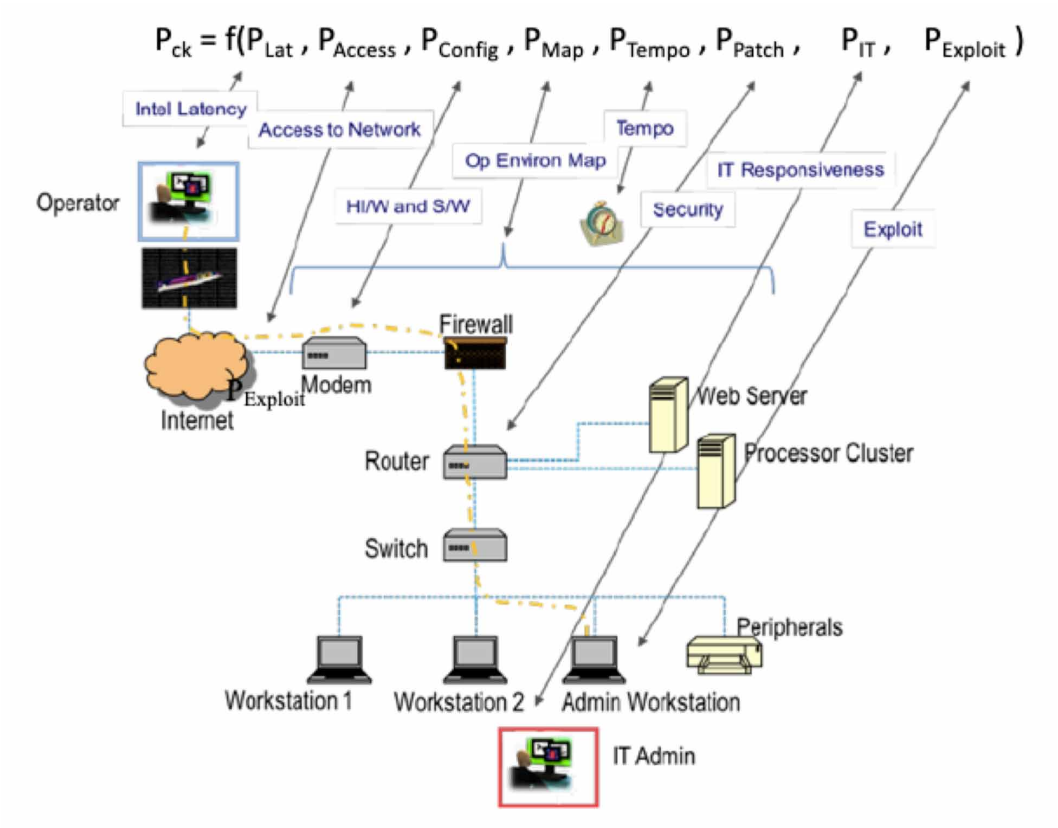
$$P_{ck}= f(P_{Latent}, P_{Access}, P_{Config}, P_{Map}, P_{Tempo}, P_{Patch}, P_{IT}, P_{Exploit}) \tag{1}$$

where:

- P_{Latent}, $P_{Access,}$ P_{Config}, P_{Map}, and P_{Tempo} are the probabilities based on the intelligence gathered on the latency of information, access points, hardware and software configurations, completeness of network map, understanding of operations tempo.
- P_{Patch} and P_{IT} are probabilities based on the likelihood of those vulnerabilities being exploited are patched and I.T.'s ability to detect and respond to the delivery of the cyber payload.
- $P_{Exploit}$ is the probability that the payload will achieve the desired mission effects.

Figure 2 shows how the probability of equation (eqt 1) may be mapped with the components of a common network. For example, the probability that the payload will achieve the desired mission

Figure 2. Cyber-Kill equation for a hypothetical network (adapted from Pinto and Zurasky, 2020)



effects ($P_{Exploit}$) may be partially or completely determined by system administrators' policy on patching and updating various software and hardware in the network. Such information may be residing on the Admin Workstation components of a network, as shown in Figure 2.

SYSTEMS MODELING: SYSML AND SECML

Systems Engineering (S.E.) is the formalized use of models as a support for the activities of analysis, design, verification, and validation (INCOSE, 2010). NASA (2019) defined S.E. as "a methodical, multi-disciplinary approach for the design, realization, technical management, operations, and retirement of a system." S.E. tends to identify, decompose, and organize the system's requirements (Leonard, J. 1999; SSEITS, 2007). Systems Modeling serves as the backbone of model-driven systems engineering since it depicts the needs of the system, the functions performed by the system, its requirements, and constraints. A modeling language with an alphabet, syntax, and semantics is used for this purpose. Lately, Systems engineering approaches have been utilized in addressing cybersecurity challenges.

SysML (Systems Modeling Language) is a specific modeling language in the field of systems engineering that allows the specification, analysis, design, verification, and validation of many systems (Delligatti, 2013). Originally, SysML was developed as part of an open-source specification project and includes an open-source license for its distribution and use. Moreover, SysML is defined as an extension of a subset of Unified Modeling Language (UML) (Hause, 2006). The models proposed in this study are developed in SysML 1.5.

Lately, there have been limited studies in modeling language for the cyber realm. For instance, Easttom (2019) emphasized the importance of improving cybersecurity with a particular security modeling language and proposed Security Modeling Language (SecML), developed from SysML to present security requirements and design both cyber-attack situations as well as defense circumstances. In the "*Internet and Wireless Security*" book, the authors cited the main objectives of SecML, which are 1) to provide constructive visual modeling language, 2) to give a sophisticated basis to evaluate the security system, 3) to depict the security requirements linkages of a system, and 4) to ensure flexibility among different levels of abstraction. Using SecML, users depict systems as a collection of components holding related attributes. In this context, Holm et al. (2013), proposed a quantitative cybersecurity analysis tool known as the Cyber Security Modeling Language (CySeMol). CySeMol permits individuals to design models and compute the likelihood of cyber-attacks. As mentioned previously, SecML is an adapted version of SysML in the cybersecurity field. In this paper, SysML will be used as modeling language in the cybersecurity domain to identify security requirements and cyber defense strategies during cyberwar operations. In traditional systems engineering, a use-case diagram describes a systems' functions and how users interact with those functions to achieve goals. The SecML equivalent would be a Misuse-case diagram, where threats or abusers introduce or download data to the system for nefarious intent. This Misuse-case diagram would provide the system designers with focus areas for designing countermeasures to combat the attackers on the system. The development of such a Misuse-case diagram would follow a similar process as a Failure Modes and Effect Analysis (FMEA). The potential vulnerabilities, or failures, could be identified and driven down to the root component of the system for added security features for the identified attack vectors. Other diagrams for visually representing conceptual, physical, and informational components of a system are block diagrams, activity diagrams, parametric diagrams, etc.

ENHANCED CYBERWEAPONS EFFECTIVENESS METHODOLOGY

This section describes how particular tools and methods in SysML may be used to enhance the previously proposed Cyberweapons Effectiveness Methodology, particularly Failure Modes and Effects Analysis (FMEA), use-case diagram, block diagram, activity diagram, and parametric diagram.

Failure Modes and Effects Analysis (FMEA)

The many components of a Failure Modes and Effects Analysis (FMEA) lends themselves to various phases of the cyberweapons effectiveness methodology. The FMEA process identifies potential failure modes, characterizes the severity and likelihood of such a failure, assesses the detection probability, and identifies prevention controls or design changes. All this information from FMEA could feed into supporting a more robust weapons effectiveness estimate. In the following paragraphs, the methodology will be discussed with the application of data to an FMEA.

The failure modes or top-level system effects in FMEA can serve as the cyberweapons damage criteria (phase 1). As shown in Table 1, damage criteria such as data modification could be identified as a potential failure mode for the system that would interrupt or disturb normal operations. Given the interfaces and data flow within the system, this can identify potential points of intrusion or failure within the data flow paths (phase 2). The identified vulnerabilities provide a baseline starting point for a full FMEA. These vulnerabilities are the root cause of the system failure modes. For instance, backdoors and hardcoded passwords are intrusion points that a cyberweapon could use to infiltrate the system to modify the data flowing within the network (phase 3). Given these root causes, the cyberweapons analysts can focus on the subsystem and component levels in the system hierarchy to assess the likelihood and severity of such a breach while investigating mitigation options (phase 4).

Use Case Diagram

To show how SysML can enhance cyberweapons effectiveness, this paper develops a use-case diagram (UCD) to model agents or stakeholders and the services they provide to the system (Friedenthal et al., 2014). The use-case diagram illustrated in Figure 6 displays how the functional users, defenders, decision-makers, information sharing security, and even the attacker interact with the network system in a cyber warfare context. For instance, the defender's end goal is to defend the network from potential cyber weapon/attacker. Defenders dedicate their resources to identify and analyze potential threats to the network (Brown et al., 2015). Defenders are modeled using actors in SysML. The information-sharing security also plays a part in the cybersecurity of the system, as it gathers cyber information about the cyberweapon and the attacker and shares this information with the appropriate stakeholders (Brown et al., 2015).

The UCD can enhance Target/Asset Assessment (phase 2) by providing cyberweapons analysts the visualization of systems actors and their possible goals when they interact with the target/asset network – in particular, it can show cyberweapons analysts how the target/asset may be defended against a specific cyberweapon and hence, adjust their choice of weapon accordingly.

Block Diagram

Furthermore, the hypothetical network presented in Figure 2 can be modeled using SysML to represent structural and behavioral features of a system using appropriate SysML diagrams. To capture both the system's hierarchy and interconnection, this paper develops a block definition diagram (BDD) and an internal block diagram (IBD). Figure 3 refers to a BDD of different entities making up a network. The network is developed from a list of components that are represented using a block, including firewall, modem pools, operator, Internet, etc.

To display the interconnections between the network's components, an IBD is used to complement the view presented by the BDD. Figure 5 is a representation of the interconnections between the different network components. The IBD allows the visualization of the internal connections between the parts of the system and shows the flow among entities (Delligatti, 2013). As an example, and illustrated in Figure 5, the internet block sends ISP information to the modem pools, which, in return, provides a digital signal to be filtered by the firewall. The firewall will then send filtered data to the router. The data is then distributed through a switch to various workstations. The information conveyed by an IBD is key to understanding the connections between the different system components.

Figure 3. Sample use-case diagram for network cybersecurity

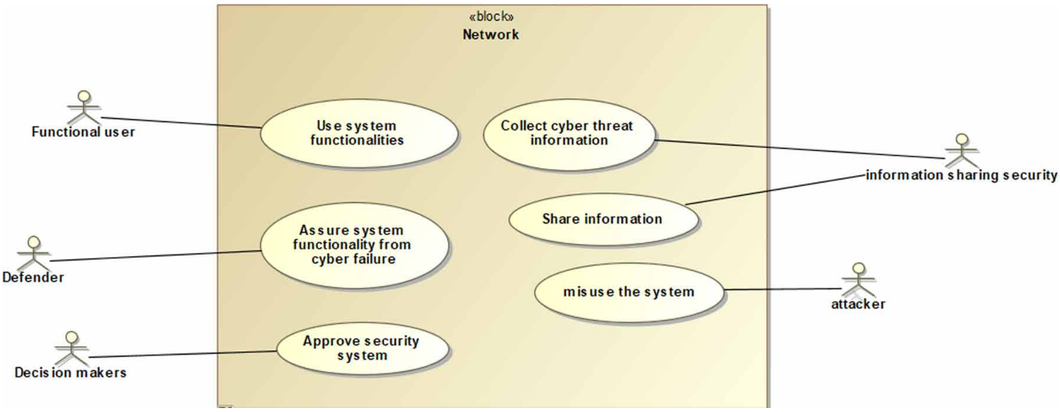

«block»
Network
Functional user
Use system functionalities
Collect cyber threat information
information sharing security
Share information
Assure system functionality from cyber failure
Defender
misuse the system
attacker
Approve security system
Decision makers

Figure 4. Block definition diagram (BDD) representation of a hypothetical network

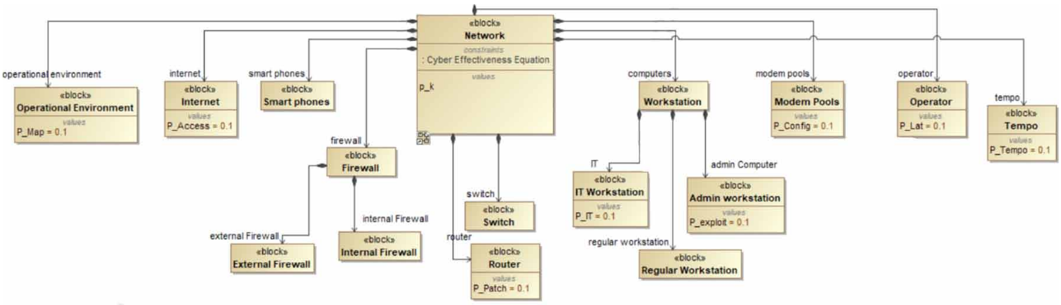
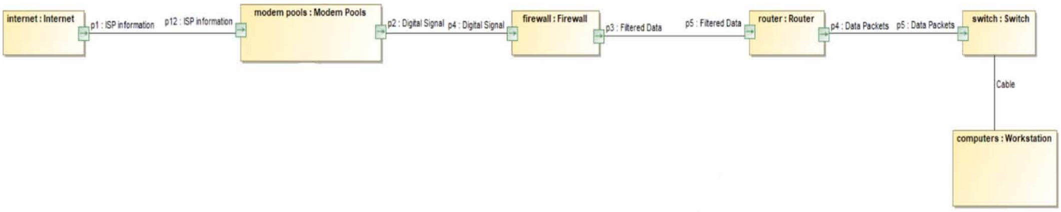


Figure 5. Internal block diagram (IBD) representing the internal connections of a hypothetical network

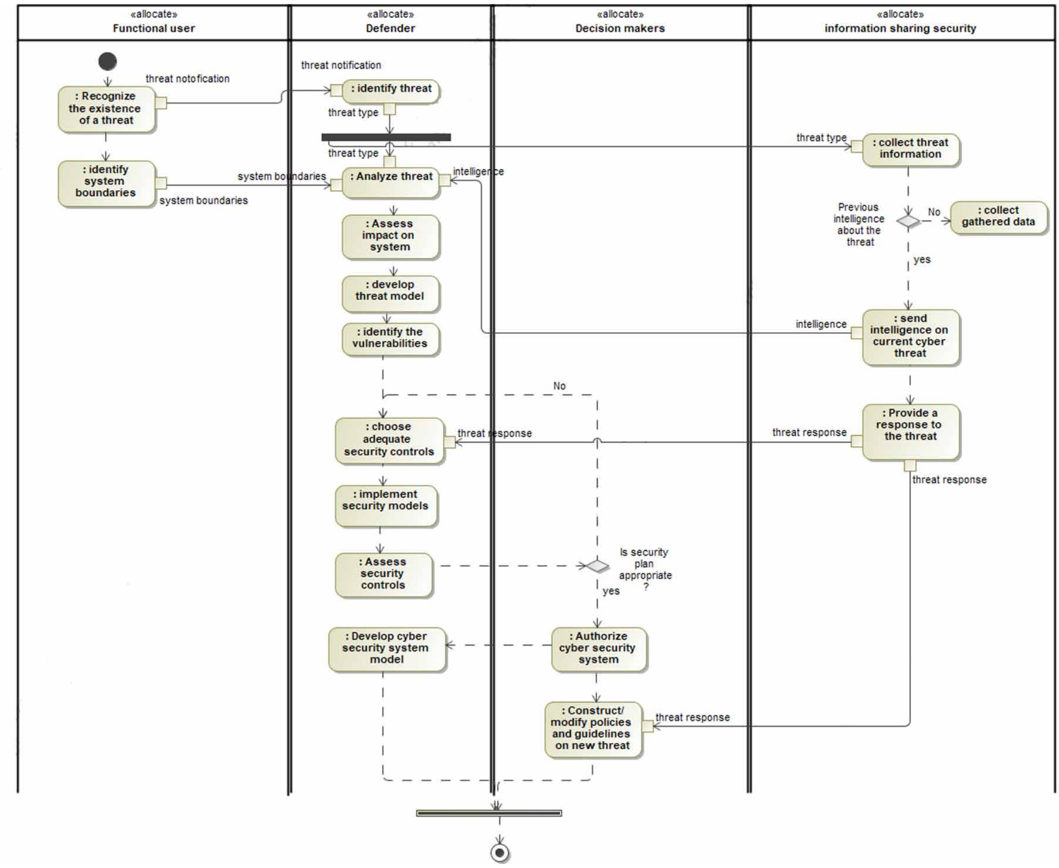


A cyberweapons analyst can use appropriate combinations of BDD's and IBD's in target/asset assessment (phase 2) to assess a specific network given a specific cyberweapon infiltration path, or conversely to pair a specific weapon to a target/asset with known weak infiltration path.

Activity Diagram

Activity diagrams (A.D.) are one of the behavioral diagrams of SysML that convey a sequence of behavior (or activities) of stakeholders and works in combination with the use-case diagram. Figure 6 displays how cyber information is being shared among four stakeholders, including functional user, defender, decision-makers, and information sharing security. As illustrated in Figure 6, the functional user may recognize the existence of a threat and communicates the information to the defender. The

Figure 6. Activity diagram displaying the information sharing process in a cybersecurity context


«allocate»
Functional user
«allocate»
Defender
«allocate»
Decision makers
«allocate»
information sharing security
threat notofication
: Recognize the existence of a threat
: identify system boundaries
system boundaries
threat notification
: identify threat
threat type
threat type
system boundaries
: Analyze threat
intelligence
: Assess impact on system
: develop threat model
: identify the vulnerabilities
No
: choose adequate security controls
threat response
: implement security models
: Assess security controls
Is security plan appropriate ?
yes
: Develop cyber security system model
: Authorize cyber security system
: Construct/ modify policies and guidelines on new threat
threat response
threat type
: collect threat information
Previous intelligence about the threat
No
: collect gathered data
yes
intelligence
: send intelligence on current cyber threat
threat response
: Provide a response to the threat
threat response

defender's role is to both identify and analyze the cyberthreat. The information-sharing security gathers intelligence of the existing threat and sends information on the current cyberthreat to the defender (Brown et al., 2015). The defender would use the information received from the information-sharing security to analyze the threat and develop an adequate model to overcome the threat. Decision-makers are involved with the authorization of cybersecurity measurements to construct new guidelines on the handling of similar cyberthreats (Brown et al., 2015).

A cyberweapons analyst can use such an activity diagram to enhance Target/Asset Assessment (phase 2) by having more insights on how the target/asset may be attacked/defended, with a particular type of weapon in mind. Eventually, the use of FMEA, UCD, BDD, IBD, and A.D. can all enhance Cyberweapons Characterization (phase 3) by pooling together reconnaissance information including network mapping, agent identification, and activities, and infiltration paths to gain lateral movement.

Parametric Diagram

Recall the effectiveness equation (Eqt. 1) from the previous section, and again shown below for convenience:

$$P_{ck}= f(P_{Latent}, P_{Access}, P_{Config}, P_{Map}, P_{Tempo}, P_{Patch}, P_{IT}, P_{Exploit})$$

The equation's variables can be mapped through the hypothetical system using SysML modeling and shown in Figure 7. In this example, a parametric diagram (P.D.) was developed to represent the Cyber effectiveness equation of a hypothetical network. The parametric diagram displays the connections between mathematical rules (aka constraint blocks in SysML) given by the cyber effectiveness equation and the different value properties (Douglass, 2015). The value properties represent the different probabilities explained in earlier sections. During the design of the system as components, or subsystems, are selected, the parametric analysis allows for characterizing the system's performance based on the parameters of the constituent components. As shown in Figure 2, P_{access} relates to the connection of the modem to the Internet. Adding additional protection within this link will modify the parameters for this variable. Choosing the best modem and authentication protocols will enhance the security of the system. The parametric modeling within SysML can quickly run the analysis to provide a system-level assessment of the P_k value. Parametric diagrams combine both design and analysis, for instance, for complex computations or algorithms, the SysML model can output parameters to mathematical software, such as Matlab, and return values based on a predefined program. This allows for integration with the engineering analysis and design tools within the model. Because P.D. can be used in conjunction with different simulation tools (Mhenni,2014), it may allow cyberweapons analyst to perform trade or scenario analyses (Douglass, 2015), such as various pairings of cyberweapons with various propagation paths and damage effects within a very short amount of time appropriate to the tempo of the cyber operation.

Overall, various techniques in SysML have been shown to enhance various phases of cyberweapons effectiveness methodology. Figure 8 summarizes the significant enhancement brought by FMEA, UCD, BBD, IBD, A.D., and P.D. to the various phases of the methodology (shaded cell).

CHEMICAL WEAPONS FACILITY CASE STUDY

This section is an adaptation of a case study from Pinto and Zurasky (2020) with supplements to show how cyberweapons effectiveness methodology can be enhanced with SysML techniques described in earlier sections. This example centers around a hypothetical scenario partly based on the vulnerability of the ABB Power Generation Information Manager (PGIM), identified as CVE-2019-18250 (CVE, 2019), and described in Kovacs (2019).

Cyber Offense

Phase One: Identification and definition of cyber damage effects

In early November of 2019, a chemical weapons facility in an undisclosed location was identified as a target for a cyberweapon with the desired damage effect of gradual interruption of its operation

Figure 7. Parametric diagram representing the cyber effectiveness equation

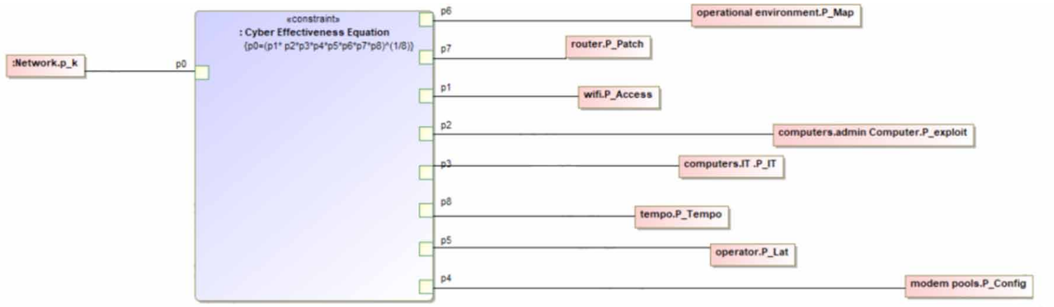
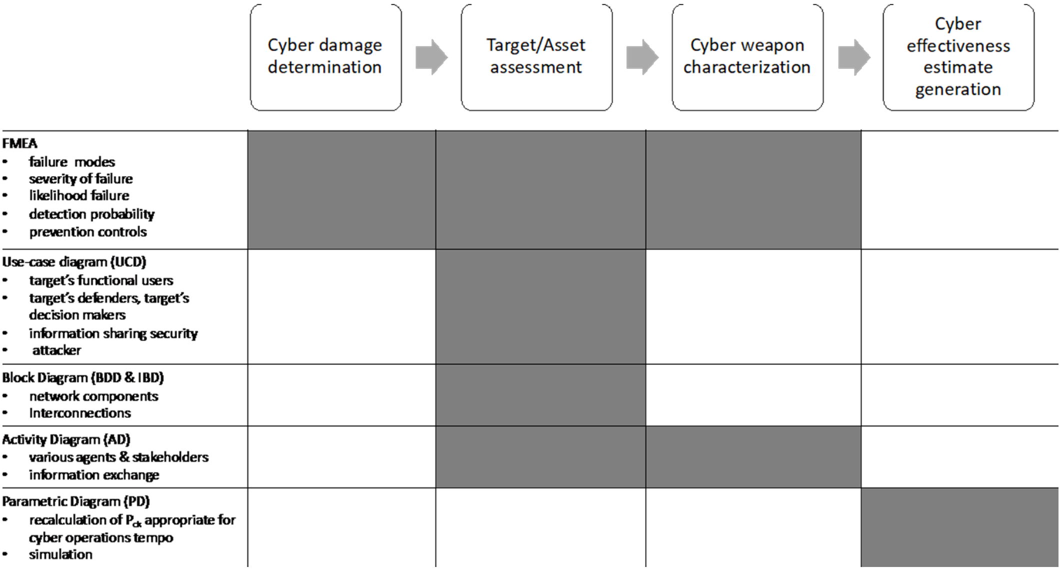


Figure 8. Summary of enhancement brought by SysML to cyberweapons effectiveness methodology



	Cyber damage determination	Target/Asset assessment	Cyber weapon characterization	Cyber effectiveness estimate generation
FMEA • failure modes • severity of failure • likelihood failure • detection probability • prevention controls	▨	▨	▨	
Use-case diagram (UCD) • target's functional users • target's defenders, target's decision makers • information sharing security • attacker		▨		
Block Diagram (BDD & IBD) • network components • Interconnections		▨		
Activity Diagram (AD) • various agents & stakeholders • information exchange		▨	▨	
Parametric Diagram (PD) • recalculation of P_{ck} appropriate for cyber operations tempo • simulation				▨

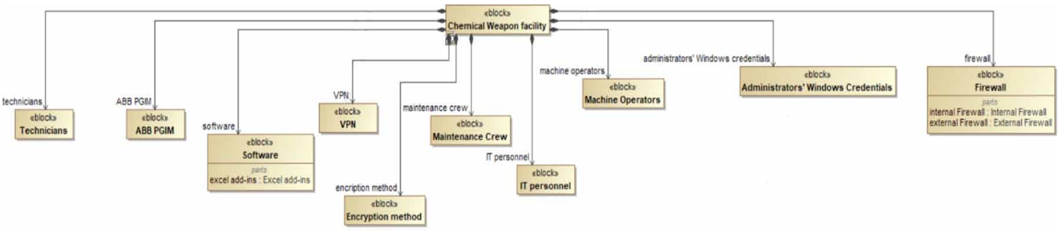
lasting at least 24 hours. The cyberweapon of choice is malware with a payload to inject incorrect equipment control information, i.e., MisI24 from Table 1.

Phase Two: Cyberthreat assessment

After the threat was identified and the desired damage effect was determined, intelligence was gathered through various ways to model the chemical weapons facility using SysML. A BDD was used to show the different entities composing the facility (Figure 9) with the main blocks composing the chemical weapon facility. This hierarchical view of the facility helped the weapons analysts visualize the target network. Significant information is summarized as follows:

- The facility uses ABB Power Generation Information Manager (PGIM) 800xA systems version 5.x, a distributed, open client/server architecture for collecting, archiving, and consolidating data from various equipment.
- Excel add-ins are used to performs basic arithmetic functions (e.g., water/steam chart calculations) used by machine operators, technicians, and maintenance crew.
- The administrators' Windows credentials are the same as the ones for PGIM.

Figure 9. BDD displaying the chemical weapon facility



Phase Three: Cyberweapon characterization

After target assessment, cyber reconnaissance was conducted, and the following significant information was gathered:

- There is only one information network for the entire facility.
- The encryption method used in transmitting information is outdated.
- The network is behind a weak firewall.
- Access into the network from the outside is through VPN but is not strictly enforced.
- The facility always employs two I.T. personnel using outdated scanning methods.

Based on this information, an FMEA was developed in SysML to assess the failure modes linked to the chemical weapon facility. Four components were considered for the FMEA including, ABB PGIM, VPN, firewall, and encryption method, as shown in Figure 10. Both effects and causes of failures were assessed based on the case study. SysML allowed the use of integrated reliability tools to facilitate the performance of FMEA analysis and its integration throughout the entire reconnaissance period.

A zero-day vulnerability (ZDV) for all versions of ABB Power Generation Information Manager (PGIM) was identified, which makes a network using PGIM vulnerable to authentication bypass, which may allow an attacker to remotely bypass authentication and extract credentials from the affected device. Being a ZDV, this vulnerability is not known to the public and has no known patch. Because threat assessment showed that the facility's PGIM credentials are the same as the Windows domain administrator credentials, it was determined that the path for lateral movement in the network would be to snoop these credentials.

A team of coders then developed and tested an exploit code on ABB 800xA systems version 5.x which bypasses authentication and default security architecture to reveal usernames and passwords in the system. With the target assessment from the previous phase and a cyberweapon in mind (i.e., the exploit code) the severity (S), occurrence (O), and detection(D) scores were then estimated and implemented based on the chemical weapon facility system, as shown in Figure 10. The risk priority number (RPN), which is given by the multiplication of the S, O, and D scores, is then automatically calculated to provide the weapons analyst with the component with the highest priority failure and provide information on critical failure modes that may match the desired damage. Defensive measures which may be encountered upon deployment of the cyberweapon are then identified (Dhillon, 1999).

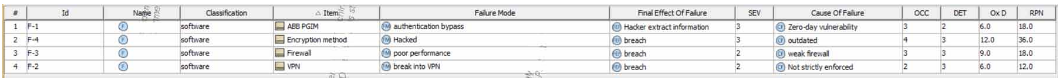
Phase Four: Cyber effectiveness estimate generation

For simple illustrative purposes, the probabilities may be expertly judged to be low (0.01), moderate (0.05), and high (0.1) based on the preceding phases. These values are summarized in Table 3.

The function of $P_k = f(*)$ used is a modified version proposed by Zurasky (2017) where the 8-th root is obtained to make very small numbers more user-friendly.

$$P_{ck} = \sqrt[8]{\left(\mathrm{PLatent}\ x\ \ \mathrm{PAccess}\ \ x\ \mathrm{PConfig}\ x\ \mathrm{PMap}\ x\ \mathrm{PTempo}\ x\ \ \mathrm{PPatch}\ x\ \ \mathrm{PIT}\ \ x\ \mathrm{PExploit}\right)}$$

Figure 10. FMEA Table



#	Id	Name	Classification	Item	Failure Mode	Final Effect Of Failure	SEV	Cause Of Failure	OCC	DET	O x D	RPN
1	F-1	F	software	ABB PGIM	authentication bypass	Hacker extract information	3	Zero-day vulnerability	3	2	6.0	18.0
2	F-4	F	software	Encryption method	Hacked	breach	3	outdated	4	3	12.0	36.0
3	F-3	F	software	Firewall	poor performance	breach	2	weak firewall	3	3	9.0	18.0
4	F-2	F	software	VPN	break into VPN	breach	2	Not strictly enforced	2	3	6.0	12.0

Table 3. Cyber effectiveness estimates for chemical weapons facility example

$\mathbf{P}_{\mathbf{Latent}}$	High; Information is very current	0.1
$\mathbf{P}_{\mathbf{Access,}}$	High; VPN not strictly enforced	0.1
$\mathbf{P}_{\mathbf{Config}}$’	High; well documented, based on manufacturer setting; single network	0.1
$\mathbf{P}_{\mathbf{Map}}$’	High; well documented; weak firewall	0.1
$\mathbf{P}_{\mathbf{Tempo}}$	High	0.1
$\mathbf{P}_{\mathbf{Patch}}$	High; no patch exists	0.1
$\mathbf{P}_{\mathbf{IT}}$	Moderate; only two personnel are employed using outdates scanning methods	0.05
$\mathbf{P}_{\mathbf{Exploit}}$	High; exploit code is tested and verified	0.1

Hence, from Table 3, the resulting $P_{ck} = \sqrt[8]{5x10^{-9}} = 0.09$

At this point, the cyberweapons analyst may iterate through the phases of the cyberweapons effectiveness methodology until the desired P_{ck} is attained.

Cyber Defense

This section briefly describes how the proposed enhanced cyberweapons effectiveness methodology may be applied for defensive purposes through the extension of the earlier chemical weapons facility scenario – now as an asset to be defended rather than as a target to be attacked.

By late November 2019, the vulnerability of PGIM was revealed publicly by Kovacs (2019). As a response, the chemical weapons facility, the network's I.T. personnel used SysML tools and techniques to develop their own FMEA, BBD, IBD, A.D., and P.D. to estimate their assessed P_{ck}, assuming that the facility needs to be defended against exploits of the ZDV meant to disrupt the operation of the facility. This P_{ck} estimated by the 'defender' most probably will not be the same as that of the P_{ck} estimated by the 'attacker' because of the differences in the information they have. At the minimum, the 'defenders' may decide to immediately apply generally known mitigation strategies. These strategies are summarized in the following:

- Segmenting the chemical production network into several networks instead of a single network for the entire facility and layered security architecture was implemented to slow down lateral movement into these networks.
- Implementing stricter access to PGIM using stronger firewall and more secure VPN to prevent unauthorized access from outside of the network.
- Windows domain user credentials were removed from PGIM.
- I.T. personnel was increased, and more advanced intrusion scanning and detection technologies were implemented, and various profiles of possible exploit codes made public (e.g., GITHUB, 2019) were analyzed by I.T. personnel for faster identification if an intrusion occurs.

Using hypothetical numbers for comparison, we summarized the resulting effectiveness estimate in Table 4.

The resulting $P_{ck} = \sqrt[8]{5x10^{-13}} = 0.03$ after mitigation strategies can be compared with that prior to application of strategies, and it is expected that the defense strategies may result in to decrease in cyber effectiveness estimate. More interestingly, the attackers may also update their own P_{ck}, now knowing that the target network has implemented the mitigation strategies. In the same way that the attacker can simulate various weapons, the defender can simulate various cybersecurity risk mitigation strategies with the aid of a parametric diagram (P.D.) until an acceptable P_{ck} is reached.

Table 4. Cyber effectiveness estimates for chemical weapons facility example (defense)

$\mathbf{P}_{\mathbf{Latent}}$	High; Information is very current	0.1
$\mathbf{P}_{\mathbf{Access,}}$	Low; VPN now strictly enforced; Windows administrators' credentials removed from PGIM; more secure firewall	0.01
$\mathbf{P}_{\mathbf{Config'}}$	Low; hardware and software settings not default and unknown to outside	0.01
$\mathbf{P}_{\mathbf{Map'}}$	Moderate; network is segmented, and security is layered	0.05
$\mathbf{P}_{\mathbf{Tempo}}$	High	0.1
$\mathbf{P}_{\mathbf{Patch}}$	High; no patch exists	0.1
$\mathbf{P}_{\mathbf{IT}}$	Low; increased I.T. personnel and monitoring	0.01
$\mathbf{P}_{\mathbf{Exploit}}$	Low; exploit code known and can be easily detected	0.01

CONCLUSION

The aim of this paper was to enhance the cyberweapons' effectiveness methodology developed by Pinto and Zurasky (2020) through the utilization of different SysML diagrams for better consistency and improvement for the cyberweapon evaluation accuracy. The proposed cyberweapon effectiveness methodology has brought a parallel but distinct process from that of kinetic weapons bringing cyberweapons analysts closer to fully integrating cyberweapons into any missions to attack a target or to defend an asset. Consistent with this parallel approach, the selection of SysML was shown to enhance various phases of the proposed cyberweapons effectiveness methodology. Most enhancements were brought onto the Target Assessment phase, while FMEA was the single technique that enhanced the greatest number of phases. Nonetheless, there is still a large area in systems modeling that needs to be explored to fully implement the proposed cyberweapons effectiveness methodology.

Future research should focus on advancing and expanding the capabilities described in this paper. Warfare is a multi-domain, highly strategic operation that must carefully coordinate the various attack and defense vectors. Supporting advancement and expansion of this framework, we proposed a research agenda that includes the following suggested topics:

- *Advancing SysML/SecML:* Additional cyber-specific components in the SysML/SecML toolbox, such as vulnerability tables that can be mapped to system components and protocol identification and documentation tables.
- *Effectiveness lexicon:* Development of a common lexicon for effectiveness assessments that support the multi-domain (cyber, directed energy, kinetic) integration of existing assessment tools.
- *Effectiveness comparisons:* Compare effectiveness predictions for a cyber tool (which may address Denial of Service, Misinformation, Data Modification, Data Repudiation, Spoofing, or Network Enumeration with their respective effects and durations) with kinetic effects (which occur instantly with effects of various lengths) or with directed energy effects (based upon a time-to-effect with similarities to kinetic damage mechanisms).
- *Multi-Domain Effectiveness:* How can the cyberweapons effectiveness assessment be integrated with existing kinetic or directed energy weapons effectiveness assessments to develop a multi-domain effectiveness model for use in mission planning?
- P_k *Optimization:* Given a common lexicon and integration of multi-domain tools, can the effectiveness of the various weapon families be compared to support the selection of a targeted attack or tailored multi-modal attack based on the highest probability of kill, P_k .
- *Defensive Vulnerability Assessment:* Using the cyberweapon effectiveness assessment to assess threat cyberweapons on friendly targets/assets to enhance defensive postures and reduce the enemy's probability of cyber kill, P_{ck}.

This paper presented an adapted framework for integrating cyberweapons effectiveness assessment into the systems engineering process and systems modeling to improve system design with respect to cyber vulnerabilities. The early development of these effectiveness estimates and identified vulnerabilities will provide the supporting analyses to design a system with reduced the likelihood of intrusion from the defensive perspective or improved probability of kill for offensive weapons. The integration of this assessment with SysML allows for integration with other domains to develop a System of Systems (SoS) level modeling approach to support mission planning.

REFERENCES

Bayuk, J. L., & Horowitz, B. M. (2011). An architectural systems engineering methodology for addressing cyber security. *Systems Engineering*, *14*(3), 294–304. doi:10.1002/sys.20182

BBC News. (2010). *Royal Navy website attacked by Romanian hacker*. Retrieved from https://www.bbc.com/news/technology11711478

Brown, S., Gommers, J., & Serrano, O. (2015, October). From cyber security information sharing to threat management. In *Proceedings of the 2nd ACM workshop on information sharing and collaborative security* (pp. 43-49). Academic Press.

Friedenthal, S., Moore, A., & Steiner, R. (2014). *A practical guide to SysML: The systems modeling language*. Morgan Kaufmann.

CVE. (2019). *CVE-2019-18250*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18250

Dark Reading. (2010). *U.S. Army Website Hacked: SQL injection, plain-text passwords leave databases exposed.* Retrieved from https://www.darkreading.com/risk/us-army-website-hacked-/d/d-id/1132749

Delligatti, L. (2013). *SysML distilled: A brief guide to the systems modeling language*. Addison-Wesley.

Dhillon, B. S. (1999). *Engineering Maintainability: How to Design for Reliability and Easy Maintenance*. Gulf Professional Publishing.

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions*, *35*(2), 291–300. doi:10.1007/s10669-015-9540-y

Douglass, B. P. (2015). *Agile systems engineering*. Morgan Kaufmann.

Easttom, C. (2019, October). SecML: A Proposed Modeling Language for CyberSecurity. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1015-1021). IEEE. doi:10.1109/UEMCON47517.2019.8993105

Gonsalves, A. (2014). *Microsoft patch fixed I.E. flaw used against U.S. military, for CSO*. Retrieved from https://www.csoonline.com/article/2607297/microsoft-patch-fixed-ie-flaw-used-against-u-s-military.html

Hause, M. (2006, September). The SysML modelling language. In *Fifteenth European Systems Engineering Conference* (*Vol. 9*, pp. 1-12). Academic Press.

Holm, H., Sommestad, T., Ekstedt, M., & Nordströ, M. L. (2013, June). CySeMoL: A tool for cyber security analysis of enterprises. In *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)* (pp. 1-4). IET. doi:10.1049/cp.2013.1077

INCOSE. (2010). Systems engineering competencies framework. Ilminster.

InfoSec. (2011). *Buffer overflow vulnerability identified in Sielco Sistemi SCADA system*. Retrieved from https://www.infosecurity-magazine.com/news/buffer-overflow-vulnerability-identified-in/

Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO CCD COE Publications.

Kovacs, E. (2019). Vulnerability in ABB Plant Historian Disclosed 5 Years After Discovery. *Security Week*. https://www.securityweek.com/vulnerability-abb-plant-historian-disclosed-5-years-after-discovery

Leonard, J. (1999). *Systems engineering fundamentals*. Defense Systems Management Coll.

Lockheed Martin. (2020). *The Cyber Kill Chain*. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#

Mhenni, F., Choley, J. Y., Penas, O., Plateaux, R., & Hammadi, M. (2014). A SysML-based methodology for mechatronic systems architectural design. *Advanced Engineering Informatics*, *28*(3), 218–231.

NASA. (2019). *Fundamentals of Systems Engineering*. Retrieved from https://www.nasa.gov/seh/2-fundamentals

Paganini, P. (2014). *Operation Pawn Storm is targeting military, government and media agencies, for Security Affairs.* Available at: https://securityaffairs.co/wordpress/29517/cyber-crime/operation-pawn-storm.html

Pinto & Zurasky. (2020). Systemic Methodology for Cyber Offense and Defense. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited.

Pinto, C. A., McShane, M. K., & Bozkurt, I. (2012). System of systems perspective on risk: Towards a unified concept. *International Journal of System of Systems Engineering*, *3*(1), 33–46.

Schwartz, M. J. (2011). *Iran Hacked GPS Signals To Capture U.S. Drone, for Dark Reading*. Retrieved from https://www.darkreading.com/attacks-and-breaches/iran-hacked-gps-signals-to-capture-us-drone/d/d-id/1101882

Sood, A., & Enbody, R. (2014). *Targeted cyber attacks: multi-staged attacks driven by exploits and malware*. Syngress.

SSEITS. (2007). *An Introduction for Transportation Professionals*. Systems Engineering for Intelligent Transportation Systems. Retrieved from https://ops.fhwa.dot.gov/publications/seitsguide/seguide.pdf

Tatar, Ü., Çalik, O., Çelik, M., & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. In *International Conference on Cyber Warfare and Security* (p. 211). Academic Conferences International Limited.

The Guardian. (2016). *SS7 hack explained: what can you do about it?* Retrieved from https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snoopingtexts-calls

The Maritime Executive. (2017). *Tests Show Ease of Hacking ECDIS, Radar and Machinery*. Retrieved from https://www.maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery

TURCK CVE. (2012). Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-12706/Turck.html

Warner, J.S., Johnston, R.G., & Alamos, C.L. (2012). *A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing*. Academic Press.

Zurasky, M. W. (2017). *Methodology to perform cyber lethality assessment* (Dissertation).

C. Ariel Pinto is an Associate Professor of Engineering Management and Systems Engineering at Old Dominion University. His works focus on multi-disciplinary approaches to risk management in engineered systems and systems engineering, and spans more than 20 years. He has written two books in Risk Analysis & Management which are currently the textbook of choice at several US universities. In 2010, he established Emergent Risk Initiative (ERI) at Old Dominion University with active members from various universities and non-academic institutions.

Matthew Zurasky is a JTCG/ME Navy Service Lead at the Naval Surface Warfare Center Dahlgren Division.

Fatine Elakramine is a Graduate Student at the Department of Industrial and Systems Engineering, Bagley College of Engineering, Mississippi State University.

Safae El Amrani is a Graduate Student at the Department of Industrial and Systems Engineering, Bagley College of Engineering, Mississippi State University.

Raed M. Jaradat is an Associate Professor at the Department of Industrial and Systems Engineering, Bagley College of Engineering, Mississippi State University.

Chad Kerr is a Graduate Student at the Department of Industrial and Systems Engineering, Bagley College of Engineering, Mississippi State University.

Vidanelage L. Dayarathna is a Graduate Student at the Department of Industrial and Systems Engineering, Bagley College of Engineering, Mississippi State University.