2020

Systemic Methodology for Cyber Offense and Defense

C. Ariel Pinto
Old Dominion University

Matthew Zurasky
Old Dominion University

Original Publication Citation

Pinto, C. A., & Zurasky, M. (2020). Systemic methodology for cyber offense and defense. *15th International Conference on Cyber Warfare and Security : ICCWS 2020, 12-13 March 2020, Norfolk, Virginia* (pp. 380-390). Academic Conferences & Publishing International Limited.

Systemic Methodology for Cyber Offense and Defense

C. Ariel Pinto and Matthew Zurasky
Old Dominion University, Norfolk, Virginia, USA
cpinto@odu.edu
mzura001@odu.edu
DOI: 10.34190/ICCWS.20.032

Abstract: This paper describes a systemic method towards standardization of a cyber weapon effectiveness and effectiveness prediction process to promote consistency and improve cyber weapon system evaluation accuracy – for both offensive and defensive postures. The approach included theoretical examination of existing effectiveness prediction processes for kinetic and directed energy weapons, complemented with technical and social aspects of cyber realm. The examination highlighted several paradigm-shifts needed to transition from purely kinetic-based processes and transition into the realm of combined kinetic and cyber weapons. Components of the new method for cyber weapons are cyber payload assessment, effects identification, and target assessment. The ultimate outcome of method is the 'Probability of Kill' for a cyber weapon paired with a threat and within a given situation. This probability is a function of factors such as intelligence gathered on the latency of information, access points, hardware and software configurations, accuracy and completeness of network map, understanding of operations tempo; likelihood that vulnerabilities being exploited are patched and IT's ability to detect and respond to the delivery of the cyber payload; and probability that the payload will achieve the desired mission effects. Aside from the use of this method for offensive purposes, it can also be mirrored as cyber defense and can serve as basis for developing cyber defense strategies, such as focused counter intelligence on access points, hardware and software configurations, and network map and architecture, comprehensive patching to assure most current and complete patches are deployed, and well trained and equipped IT with ability to detect and respond to cyber payloads.

Keyword: Systemic; Systematic; Offense; Defense; Risk; Effectiveness

1. Background

Offensive cyber operations (OCO) have been portrayed as an adjunct to conventional weapons and that predictable time and effect will be needed if cyber weapons are to be used as a military weapon (The Economist, 2010). Cyber weapons have also been described to impact warfare more than ordnance (United Press International, 2014). Combatant commanders and mission planners rely upon validated weapon and target information to determine the probability of success for mission scenarios by matching kinetic weapons to targets. Particularly, the Joint Munitions Effectiveness Manuals (JMEMs) provide damage probabilities for specific weapons and threats, physical and functional characteristics of munitions and weapon systems, threat vulnerability, obscuration on weapon effectiveness, and analytical techniques and procedures for assessing munitions effectiveness (U.S. Army Material Systems Analysis Activity, 2016). JMEMs allow a standardized comparison of weapon effectiveness across all three service communities – the Army, Navy, and Air Force. This provides combatant commanders a necessary capability - to determine the best combination of weapon ordnance and tactics to attack and render enemy systems and structures inoperable. These combatant commanders will not utilize cyber warfare without knowing the effects it will produce or the potential collateral damage that may occur. Hence, a similar capability for OCO is deemed necessary or the United States military will cede this aspect of warfare to adversarial parties. Plans to enable the U.S. military to conduct a "combined arms campaign across all domains – land, air, maritime, space, and cyberspace" makes it clear that there has to be shift from strictly using kinetic weapons to one that combines with cyber weapons (U.S. Department of Defense, 2012). Similar attempts have been ongoing in other parts of DoD, e.g., Air Force CyberWorkx which tries to leverage Functional Mission Analysis (FMA) to effectively transition the communication mission to the cyber mission and develop specialized skill sets required for the Air Force's Mission Defense Team operations (Collins, Chiaramonte, & McMinn, 2017).

2. Current Assessment of Kinetic Weapons

The process established to assess kinetic weapons allows an analyst to assess the physical interactions between ordnance and the threat and to determine if the resulting damage is sufficient to negate the threat's mission. The current basic process to assess kinetic weapons can be summarized in three phases: 1) threat assessment, 2) weapons characterization, and 3) damage definition.

2.1 Threat assessment

Once a threat system is identified, intelligence is collected on the threat to identify its critical system elements. A schematic model is created of the physical interconnectivities of components and, if appropriate, the significant crew members of the threat system. This model is created using combinations of tools like Fault Trees and Failure Modes and Events Analysis (FMEA). Once a desired damage level is associated with the threat, a complementary mirror model of failures for the system components is developed to indicate which components are relevant to affect the intended damage. Component vulnerabilities are estimated based on test data, computational physics hydrocode analyses, or engineering level analyses and may include use of penetration equations and specialized algorithms, e.g., Jacobs-Roslund equation for explosive detonation (Naval Surface Warfare Center Dahlgren Division, 2014).

2.2 Weapons characterization

Characterizing weapons is done using standard data collection methods appropriate to weapons' effects on the threat system and environments. Threat assessment information from the previous phase is used together with information specific to weapons, e.g., fragmentation data is collected for fragment masses, shape, velocities, and material, and penetration data is collected for projectiles and shaped charge devices. Engineering-level simulation codes may be utilized to determine the expected engagement geometry with the threat system.

2.3 Damage definition

An analyst can pair the threat with a weapon and perform an effectiveness estimate. This estimate provides a probability of damage given a hit on the threat and is dependent upon the munition characteristics, the threat vulnerability, the damage definition criteria, the velocity and orientation at impact. Examples of damage definitions is shown in Table 1 (adapted from Driels M. R., 2013).

Table 1: Examples of damage definitions

Target Type	Damage Definitions
Land Vehicles	K – catastrophic kill (not repairable); M0 – mobility kill (cannot move, immediately; M40 – mobility kill (cannot move within 40 minutes); F – firepower kill (cannot fire)
Parked Aircraft	PTO – repairs requiring at least 5 minutes; PTO4 – repairs requiring at least 4 hours; PTO24 – repairs requiring at least 24 hours
Personnel (standing)	Defense (prevent) within 30 seconds; Assault (prevent) within 30 seconds; Assault (prevent) within 5 minutes; Supply (prevent) within 12 hours

Eventually, the effectiveness of a weapon is defined as the Probability of Kill (P_K) and is the function of several probabilities, such that

$$P_k = f(P_{trk}, P_{eng}, P_{ho}, P_{disc}, P_s, P_{msl}, P_h, P_{d|h}, P_{k|d})$$

Where

- P_{trk} is the probability that the target is acquired and tracked
- P_{eng} is the probability that the target is engageable (within the weapon system performance envelope)
- P_{ho} is the probability that handover occurs between the search sensor and the fire control sensor
- P_{disc} is the probability that the weapon system can discriminate the target from decoys or clutter
- P_s is the probability that the platform or overall system (excluding weapons itself) performs reliably
- P_{msl} is the probability that the weapon will perform reliably, including propulsion, guidance, and fuzing functions
- P_h is the probability of the weapon hitting the target
- $P_{d|h}$ is the probability of damage to the target given a hit
- $P_{k|d}$ is the probability of a kill given the damage level

Simulation codes such as Advanced Joint Effectiveness Model and Effectiveness ToolBox are used to calculate these terms. Figure 1 illustrates a typical effectiveness equation for a missile intercept event (Zurasky, 2015).

$$P_k = f(P_{trk}, P_{eng}, P_{ho}, P_{disc}, P_s, P_{msl}, P_h, P_{d|h}, P_{k|d})$$

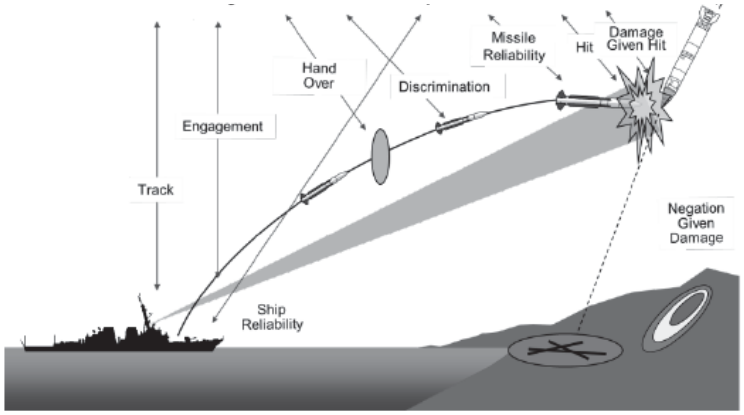

Figure 1: Kinetic System Effectiveness Kill Chain

3. Inherent Differences Between Cyber Weapons and Kinetic Weapons

Weapons can impart damage to threats through physical means such as blast, fragment penetration, and heat. For example, a high explosive blast causes injuries in the lungs, gastrointestinal tract, and ears in humans and damage in equipment compartments and manned spaces in buildings and vehicles. For laser weapons, the concentrated beam of visible or invisible light is converted to heat, increasing the temperature of a material and causing weakening and deformations.

However, cyber weapons interact with threats in a different way, as summarized in Table 2. Cyber weapons act on logical rather than physical interconnectivities of components and significant crew members. Cyber weapons allow compromise of computers and processors by identifying important data to manipulate, steal, or destroy, i.e., affects its Confidentiality, Integrity, and Availability. Cyber weapon penetration into a system is not achieved physically. Instead of exploiting the laws of physics as kinetic weapons do, cyber weapons leverage inter-computer protocols and human-in-the-loop to gain access to threat computers. Some cyber weapons engage networking and administrative tools to probe and map networks and to conduct lateral movements across networks while others manipulate the computer code to alter the output of algorithms.

Furthermore, cyber weapons do not come with an explosive charge. Instead, physical and logical damage must be created by the targeted system to itself through stopping or altering ongoing processes (Rid and McBurney, 2012). The existing definitions for mobility damage and firepower damage still apply to cyber weapons for those effects that cause physical damage. On the other hand, not all cyber weapons may be capable or designed to directly contribute to Crew damages.

Table 2: Summarized differences of kinetic and cyber weapons

	Kinetic weapons	**Cyber weapons**
Threat assessment by…	physical interconnectivities of components and significant crew members	Logical interconnectivities of components and significant crew members
Target systems penetration using…	laws of physics	inter-computer protocols, processes, and procedures; system design and architecture; human-in-the-loop; social engineering
Latency	Immediate	From immediate to indeterminate
Damage caused by…	laws of physics; physical means such as blast, fragment penetration, and heat effects	manipulation of software and information; targeted system to itself through stopping or altering ongoing processes
Damage persistence...	Various	Various
Types of damage…	Direct damage to mobility, firepower, and crew	Direct & indirect damage to mobility, and firepower; indirect damage to crew

4. Paradigm Shift to Cyber Weapons Assessment

As in the case for kinetic weapons, the objectives of a cyber weapon effectiveness and effectiveness prediction process are to promote consistency and improve weapon system evaluation accuracy across DoD. Without a proper assessment and prediction process, commanders will remain reluctant to employ cyber weapons.

Consistency is implemented through a common set of definitions and assumptions that are used by each of the Services to produce weapon system performance estimates. This commonality ensures that significant differences, if any, are attributable to the weapon system and threat characteristics rather than the methods employed by the individual Services. Also, standardization facilitates a common interpretation and meaningful comparison of weapon system performance. Thus, the predictions delivered by a cyber effectiveness analysis are likely to be accepted by the warfighting community.

Given the ever expanding and emerging cyber realm, and hence also the capabilities of cyber weapons, the effectiveness and effectiveness prediction methodology must be robust enough to be tailored to suit each analysis. That means there must be some common structure that gives the analyst leeway to develop assessments against threats and for damage effects not yet encountered.

For timely acceptance across the Services, a cyber effectiveness methodology must have some parallelisms with that for the more established kinetic weapons. However, the emerging nature of the cyber realm would necessitate a precursory phase of constant survey of potential cyber effects. Hence, a cyber effectiveness methodology may include the following phases, as shown in Figure 2: Identification and definition of cyber damage effects, Cyber threat assessment, Cyber weapon characterization, and Cyber effectiveness estimate generation.

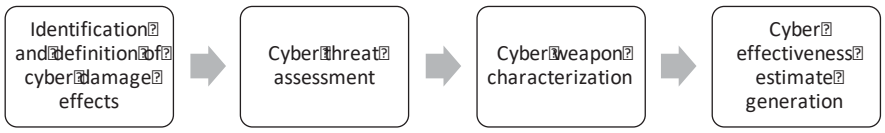

Figure 2: Proposed cyber effectiveness methodology

4.1 Identification and definition of Cyber damage effects

The first element of the common structure is an updated and common set of damage criteria. In some cases, a cyber weapon may enact effects that cause physical damage like a kinetic weapon not possible in the recent past. For example, a new asymmetrically discovered Programmable Logic Controller (PLC) vulnerability (i.e., unpublished Zero-Day Vulnerability) may allow a cyber weapon that causes a servo controller to turn off and induce the same failures to a flight system as those caused by a penetrating projectile damaging the same servo controller. However, once this vulnerability becomes symmetrically known, then effectiveness may be reduced using patches deployed to affected PLC's. This and other types of added variation in cyber effects makes the prediction of cyber weapon effectiveness problematic. The outcomes of some of these effects do not directly correspond to existing kinetic weapon damage definitions. Cyber-specific damage effects may include those listed in Table 3.

These and other possible types of effects that may emerge need to have quantifiable metrics associated with them to be usable in the field. Two important metrics both based on time are how rapid the effect sets in (latency), and the associated duration period (persistence), as shown in Table 3.

Table 3: Cyber effects, brief description, and sample metricification (adapted from Zurasky, 2017)

Cyber damage	Brief description	Sample metrics
Unavailability of network resources	Computer, communication, or network resources are made unavailable to intended users by temporarily or indefinitely disrupting services of a host connected to the Internet (e.g., 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	an attempt to masquerade as someone else	Latency: immediate Persistence: indeterminate

4.2 Cyber Threat Assessment

Like kinetic weapon assessments, a multi-phase cyber effectiveness threat vulnerability assessment must include the following: (1) threat selection, (2) threat modeling, and (3) identification of component vulnerabilities.

4.2.1 threat selection

In threat selection, the analyst will identify the threat and begin to gather baseline information. This will include a brief description of the threat, relevant photos or schematic drawings, top level failure analysis logic trees, and a list of assumptions pertinent to the analysis.

4.2.2 threat modeling

In threat modeling, the analyst will begin to develop a threat model to include a detailed description of the threat, a network model (if appropriate), and a failure modes and effects analysis (FMEA). For a cyber evaluation, the physical components of the threat are not significant. Instead, the software code and its functional elements are the items to be evaluated. The system boundaries are important when developing the network model. The key aspect of threat modeling is to identify the critical functional elements and the conditions that need to be altered in order to change the state of the threat system and achieve the desired effect. For example, the FMEA can identify a servo controller as a single point failure node. A well-designed cyber weapon can then alter the state of the servo causing loss of system control.

4.2.3 vulnerability assessment

In vulnerability assessment, the analyst will identify the vulnerability of the identified critical cyber components, including how it can be exploited, i.e., access, trigger, and impact. The vulnerability can be considered as an element (flaw or designed) in the software or environment that can be exploited. These elements (both flaws and designed) becomes vulnerabilities when exploitation path are identified. Otherwise, these may simply be inert elements. Vulnerabilities can exist in the threat system design, within installed software, within its network configuration, or be associated with its business operations. Some known vulnerabilities and actual incidents of exploitation are shown in Table 4 (adapted from Sood and Enbody, 2014).

Table 4: Cases of exploited vulnerabilities

Vulnerability Types	Description	Vulnerable Systems Examples
Backdoors and Hardcoded Passwords	hardcoded passwords embedded in the firmware that allow attackers 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 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 U.S. Veterans of Foreign Wars' website (Gonsalves, 2014) • Operation Pawn Storm uses vulnerabilities in MS 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 US or Common Channel Interoffice Signaling 7 (CCIS7) in the UK,(The Guardian, 2016) • Possible attacks to spoof GPS communication to control U.S. drones (Schwartz, 2011)

All the various cyber components must be listed with their associated vulnerabilities. This will provide the cyber weapon designer with a complete description – equivalent to the kinetic weapon Threat Geometry Model – against which to choose the most appropriate available cyber capability to cause damage.

4.3 Cyber weapon characterization

A cyber weapon is a software capability by which an attacker exploits a vulnerability within a target system to cause damage. None of the kinetic weapon characteristics apply (e.g., warhead fragmentation and blast overpressure data, guidance methods, fuse functions, and reliability). Instead, new characteristics will have to be developed. These should be categorized according to cyber weapon's functional responsibilities of Reconnaissance, Lateral Movement, Payload Deployment.

4.3.1 Cyber Reconnaissance

In order to penetrate and exploit an adversarial network, some aspect of the cyber weapon will require networking reconnaissance tools to map out the threat network, to probe potential avenues, and to monitor activities. The weapon will be required to locate the desired target components and identify ways to get to them, i.e., cyber access to exploit vulnerabilities. By utilizing host and port scan applications to map out the network resources, the weapon will develop an inventory of relevant target components. The reconnaissance characterization should include descriptions of its function and the operational environment in which it operates. Lightcyber (2016) notes that 99% of reconnaissance and lateral movement threats originated from legitimate applications and only 1% originated from malware. Some of the more popular networking and hacking reconnaissance tools include Angry IP Scanner, PingInfoView, and Nmap.

4.3.2 Lateral movement

Once the target system has been successfully penetrated, the cyber weapon may have to extend across the network to the vulnerable component. It will do so by using lateral movement applications. Lateral movement facilitates the attacker to maintain presence in the network, gain control of the administrative privileges, and move to the key vulnerable components. The lateral movement characterization should include descriptions of its function and the operational environment in which it operates. Some of the more popular administrative tools for lateral movement include SecureCRT, Putty, and BeyondExec Remote Service.

In addition, remote desktop tools are used to move laterally within a network and to remotely control elements. Legitimate Information Technology administrators use them to manage networks, but cyber weapons can use them to control elements that have been compromised. Some of the more popular remote desktop tools for lateral movement are TeamViewer, WinVNC, and Radmin.

4.3.3 Payload deployment

In addition to the reconnaissance and lateral movement functions, a cyber weapon may deploy a payload. Payload refers to the component of a computer code that executes an activity that is unwanted by the targeted system, i.e., to trigger the exploited vulnerability. This does not include the reconnaissance and lateral movement code required to get the payload packet to its destination. Some example effects of payloads are data exfiltration, manipulation or destruction, interrupted or inconsistent messages, and the delivery of spam emails through an infected user's account. The payload characterization should include descriptions of its function and the operational environment in which it operates or would remain dormant. For example, the characterization should indicate that it exfiltrates data from computers that utilize the Windows 10 operating system but will not be active in other variants of Windows OS.

4.4 Cyber offense effectiveness estimate generation

The effectiveness estimate of cyber weapons is the point in the process where the analyst predicts the outcome of the use of a weapon on a specific threat system in a specified environment, e.g., impact of vulnerability exploitation. Determining Probability of Kill (P_K) for a kinetic weapon system is often used by logisticians to determine weapon load-out and by mission planners to develop tactics. Commanders must have confidence in the effectiveness of weapons before using them, and especially important when physical damage may not be evident as confirmation.

An effectiveness equation for a typical missile intercept event was illustrated in Figure 2. It was pointed out that much of the uncertainty, and the associated probabilities, occur after the engagement begins. Similar kill chain models for cyber engagements have been previously developed by Lockheed Martin and Mandiant (now FireEye) for an advanced persistent threat (APT) attack (Holmes, 2015). In both there are distinct stages of the engagement. The durations of these stages are much longer than the stages of a kinetic engagement. In addition, the pre-compromise stage where reconnaissance occurs is actually prior to the engagement start, i.e., prior to when the commander wants to engage the cyber weapon.

The cyber equivalent to the kinetic equation in Figure 1 can be expressed as:

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

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 likelihood of that vulnerabilities being exploited are patched and IT'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 3 shows the resulting cyber effectiveness equation for a path through a hypothetical network (from Zurasky, 2017).

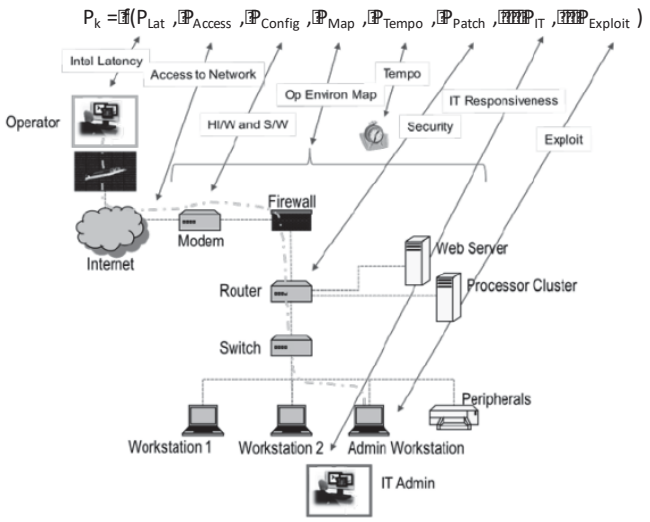

Figure 3: Cyber effectiveness equation for a hypothetical network

4.5 Example cyber offense effectiveness generation: Chemical weapons facility

This section describes an example of how the proposed cyber weapon effectiveness methodology may be applied to 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).

4.5.1 Phase 1: Identification and definition of cyber damage effects

In early November of 2019, a chemical weapons facility was identified as a threat and a desired damage effect was determined to be a gradual interruption of its operation lasting at least 24 hours by injecting incorrect equipment control information, i.e., MisI24 from Table 3.

4.5.2 Phase 2: Cyber threat assessment:

After the threat was identified and a desired damage effect was determined, intelligence was gathered through various ways. 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

4.5.3 Cyber weapon characterization

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

- There is only one information network for the entire facility
- 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 IT personnel using outdated scanning methods

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.

4.5.4 Cyber effectiveness estimate generation

For simple illustrative purpose, 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 5.

Table 5: Cyber effectiveness estimates for chemical weapons facility example

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

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-firendly.

$$P_k = \sqrt[8]{(P_{\text{Latent}} \text{ x } P_{\text{Access}} \text{ x } P_{\text{Config}} \text{ x } P_{\text{Map}} \text{ x } P_{\text{Tempo}} \text{ x } P_{\text{Patch}} \text{ x } P_{\text{IT}} \text{ x } P_{\text{Exploit}})}$$

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

5. Cyber defense effectiveness estimate generation

Anti-goal approach has been proposed as one way to create failure scenarios from a top-down approach (e.g., Pinto, Tolk, and Landaeta, 2010), and can be appropriately used to transform the cyber offense effectiveness equation into a cyber defence effectiveness equation. That is, if cyber offensive mean increasing the likelihood of cyber weapon effectiveness, maximizing Pk, then cyber defence means maximizing (-Pk), or equivalently, minimizing Pk. Hence, the defensive duality of cyber effectiveness equation is:

$$\text{Minimize } P_k = f(P_{Lat}, P_{Access}, P_{Config}, P_{Map}, P_{Tempo}, P_{Patch}, P_{IT}, P_{Exploit})$$

Broadly, this equation can be the basis for developing cyber defense strategies, such as

- Focused counterintelligence on access points, hardware and software configurations, and network map and architecture to keep adversary's P_{Latent}, $P_{Access,}$ P_{Config}, P_{Map}, and P_{Tempo} at their minima
- Comprehensive patching to assure most current and complete patches are deployed to minimize P_{Patch},
- Well trained and equipped IT with ability to detect and respond to cyber payloads to minimize P_{IT}

5.1 Example cyber defense effectiveness generation: Chemical weapons facility

This section briefly describes how the proposed cyber weapons effectiveness methodology may be applied for defensive purpose, through the extension of the earlier chemical weapons facility scenario.

By late November 2019, the vulnerability of PGIM was revealed publicly by Kovacs (2019). As a response, the chemical weapons facility applied the following cyber defense strategies as suggested by Bodforss (2019) and US-CERT (2019). 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
- More controlled access to PGIM using stronger firewall and stricter implementation of VPN for access outside of the network
- Windows domain user credentials were removed from PGIM
- IT personnel were 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 IT personnel for faster identification, if intrusion occurs

Correspondingly, the resulting effectiveness estimate – both for purpose of offense or defense - can be summarized in Table 6.

Table 6: Cyber effectiveness estimates for chemical weapons facility example (defense)

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

From Table 6, the resulting Pk $=\sqrt[8]{5x10^{-13}} = 0.03$. As expected, cyber defense strategies may result to decrease in cyber effectiveness estimate and the proposed cyber weapon effectiveness method was shown to be able applicable to both offensive and defensive purposes

6. Summary and Conclusion

A cyber weapon effectiveness and effectiveness prediction process was derived from similarities and differences between cyber and kinetic weapons, with the objective of promoting consistency and improving accuracy of weapon system evaluation across DoD. The four phases of this process are 1) Identification and definition of cyber damage effects, 2) Cyber threat assessment, 3) Cyber weapon characterization, and 4) Cyber effectiveness estimate generation. Furthermore, cyber defense strategies can be mirrored from this same offensive process, e.g., focused counterintelligence, comprehensive patching, and capable IT program.

References

BBC News (2010). Royal Navy website attacked by Romanian hacker. Available at: https://www.bbc.com/news/technology-11711478

Collins, A. (no date). *MISCELLANY: Miscellaneous Technical Articles* by Dr. A.R. Collins, online. Available at http://www.arc.id.au/RobinsOnBallistics.html [Accessed 22 Dec 2016].

Collins, J.A., Chiaramonte, M.W., & McMinn, L. (2017). Functional Mission Analysis (FMA) for the Air Force Cyber Squadron Initiative (CS I).

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. Available at: https://www.darkreading.com/risk/us-army-website-hacked-/d/d-id/1132749?

Driels, M. R. (2013). *Weaponeering*. Monterey, CA: American Institute of Aeronautics and Astronautics, Inc.

GITHUB (2019). Proof-of-Concept (PoC) for a vulnerability in ABB Power generation information manager (PGIM), https://github.com/rbodforss/pgpwner/.

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

Holmes, S. (2015). *Kill Chain Models*, online. Available at https://www.lowmanio.co.uk/blog/entries/kill-chain-models/ [Accessed 20 Feb 2017].

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

Kovacs, E. (2019). Vulnerability in ABB Plant Historian Disclosed 5 Years After Discovery, in Security Week, November 18, https://www.securityweek.com/vulnerability-abb-plant-historian-disclosed-5-years-after-discovery.

Lightcyber. (2016). *Cyber Weapons: 2016 Report*. Los Altos: Lightcyber.

Naval Surface Warfare Centre Dahlgren Division. (2014). *System Analysis Overview*.

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, C.A., Tolk, A., and Landaeta, R. (2010). *Goal approach to risk scenario identification in systems development*. 31st Annual National Conference of the American Society for Engineering Management 2010, ASEM 2010. 361-366.

Rid, T. and McBurney, P. (2012). *Cyber-Weapons*. RUSI Journal, 157(February/March), 6-13.

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

Sood, A. K., and Enbody, R. (2014*). U.S. Military Defence Systems: The Anatomy of Cyber Espionage by Chinese Hackers*. Georgetown Journal of International Affairs.

The Economist (2010, July 01), *War in the fifth domain,* online. Available at https://www.economist.com/ [Accessed 06 Oct. 2019].

The Guardian (2016). SS7 hack explained: what can you do about it? Available at: https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls

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

U.S. Army Material Systems Analysis Activity. (2016). *Joint Technical Coordinating Group for Munitions Effectiveness Program Office*, online. Available at https://web.amsaa.army.mil/JTCGMEOPO.html [Accessed 23 Dec 2016].

U.S. Department of Defence. (2012). *Sustaining Global Leadership: Priorities for 21st Century Defence*.

United Press International (2014, January 31). *Israel combats cyberattacks, 'biggest revolution in warfare'*, online. Available at http://www.upi.com/ [Accessed 05 Jan 2017].

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

Zurasky, M. (2017). *Methodology to perform cyber lethality assessment*. PhD. Old Dominion University.

Zurasky, M. W. (2015). *Lethality and Effectiveness Branch Overview*.