

SMALL WARS JOURNAL

March 11, 2018

http://smallwarsjournal.com/jrnl/art/odni-common-cyber-threat-framework-new-model-improves-understanding-and-communication

ODNI Common Cyber Threat Framework
A New Model Improves Understanding and Communication

Robert Zager and John Zager

Introduction

A Common Cyber Threat Framework: A Foundation for Communication (Cyber Threat Framework) is a new cyber security analytical framework published by the Office of the Director of National Intelligence (ODNI).[1] According to the ODNI, "its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity."[2] The Cyber Threat Framework is a vast improvement over the inconsistent lexicons which came before it. In this paper we review the Cyber Threat Framework and propose an extension to the Cyber Threat Framework which integrates cyber threats with cyber defenses.

The Common Cyber Threat Framework Overview

With So Many Cyber Threat Models or Frameworks - Why build another?

-Office of the Director of National Intelligence[3]

Acknowledging the existing body of cybersecurity frameworks, the ODNI observes:[4]

> Cyber experts couldn't easily and consistently convey what was happening on the networks to non-cyber audiences, and senior leaders couldn't readily understand the essence of what they were being told or how to put it to use in decision making.

Why build another? Quoting the ODNI:[5]

... Because comparison of threat data across models and users is problematic

Following a common approach helps to:

- Establish a common ontology and enhance information-sharing since it is easier to map unique models to a common standard than to each other
- Characterize and categorize threat activity in a straightforward way that can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalists to technical expert
- Achieve common situational awareness across organizations

The ODNI deconstructed eight existing frameworks and synthesized them into a new hierarchical approach – the Cyber Threat Framework. The Cyber Threat Framework is an innovative stage model which is abstracted from incident details. This abstraction overcomes the

institutional biases which resulted when each organization "characterized activity to meet their internal needs using their own terms, many of which had different meanings even when they used the same words."[6]

The Cyber Threat Framework stage model creates a four-layer hierarchy which is summarized in Figure 1.[7]

Cyber Threat Framework Version 4.0 Lexicon of concepts and definitions				
The Cyber Threat Framework Lexicon is meant to be a flexible and open document. Our goal is to provide enough content and guidance to allow users to appropriately and repeatably categorize data without producing a massive document covering every conceivable possibility at the "Action" and "Indicator" level. We solicit your comments and feedback on content, accuracy, and usability as a means to continually improve its content and utility. Recommended changes must be unencumbered (e.g., non-proprietary or copyrighted) as they will be shared openly.				
This is a work of the U.S. Government and is not subject to copyright protection in the United States.				
Terms				Definitions
Layer 1 Stages	layer 2 Objectives	Layer 3 Actions	Layer 4 Indicators	
stages				The progression of cyber threat actions over time to achieve objectives.
	objectives			The purpose of conducting an action or a series of actions.
		actions		Activity and associated resources used by a threat actor to satisfy an objective.
			indicators	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attempt to take or having taken an action, or to achieve an objective.

Figure 1. Cyber Threat Framework. Source: ODNI

As illustrated in Figure 2, Layer 1 "Stages" is the foundation of the Cyber Threat Framework.[8]

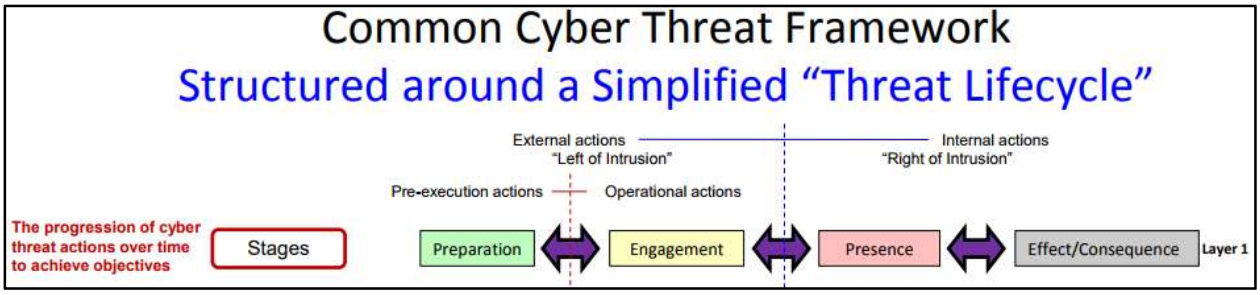


Figure 2. Cyber Threat Framework, Layer 1. Source: ODNI

Building from Stages, the Cyber Threat Framework creates a comprehensive lexicon (Lexicon). The Lexicon's definitions of the four Stages terms are:[9]

Preparation: Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.

Engagement: Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores.

Presence: Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores.

Effect/Consequence: Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.

The Stages bind the other layers (Objectives, Actions and Indicators) to time, forcing a sequential analysis of cyber threats. The four stages are divided into major divisions, Left of Intrusion and Right of Intrusion. Although not expressly stated, the boundary between Left of Intrusion and Right of Intrusion (which occurs between Engagement and Presence) is Intrusion. Intrusion is an important threat transition because pre-intrusion defensive interventions are preventative while post intrusion defenses are remedial. Similarly, Left of Intrusion is divided into two distinct phases, Pre-Execution actions, which occur in the Preparation Stage, and Operational Actions, which occur during the Engagement Stage.

While time sequencing is not unique to the Cyber Threat Framework, the hierarchical structure driven by the simplified non-technical threat progression accomplishes the stated objective of mapping diverse models to a common standard.

No doubt addressing the concern that terminology can be used to advance institutional objectives, the Lexicon is remarkably free of jargon. Figure 3 illustrates how the Lexicon describes the universe of Stages and Objectives without recourse to technical jargon.[10]

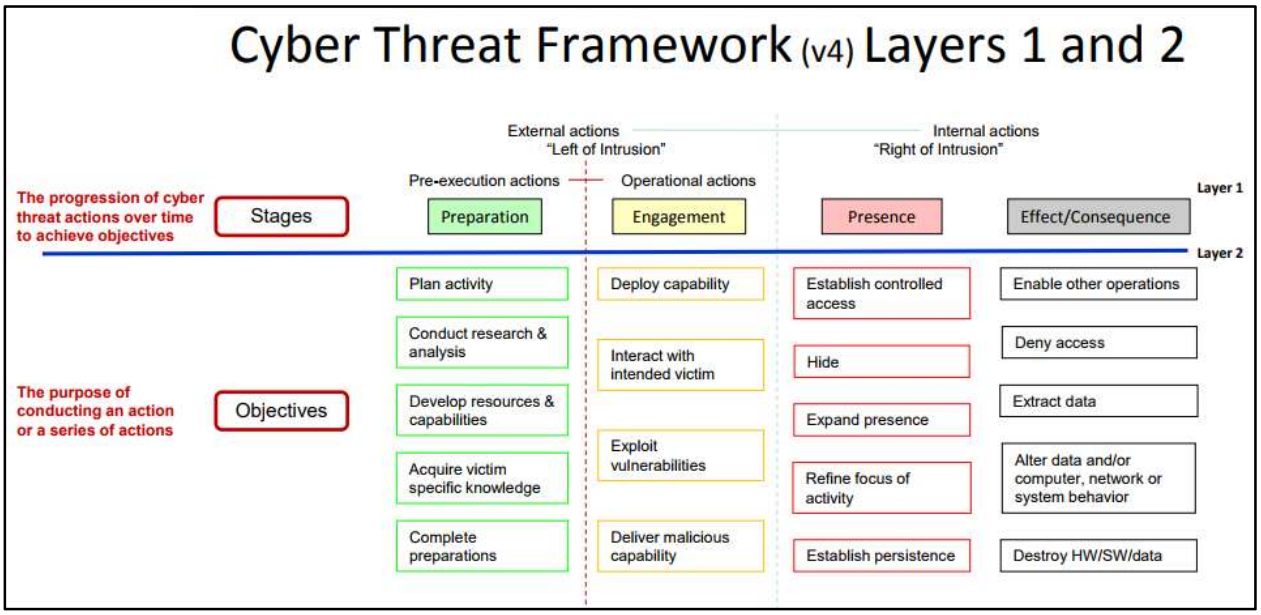


Figure 3. Cyber Threat Framework (v4) Layers 1 and 2. Source: ODNI

The Lexicon continues its use of generally used English words and phrases in the extensive Layer 3 Actions nomenclature.[11] Figure 4 is an excerpt from the Lexicon's Layer 3 Actions

nomenclature which illustrates the jargon-free description of the technically complex topic of establishing controlled access.[12]

Layer 1 Stages	Layer 2 Objectives	Layer 3 Actions	Layer 4 Indicators	Definitions
Presence	Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores			
	Establish controlled access			Activities (automated or manual) intended to gain unauthorized control (violate the confidentiality) of the intended victim's computer(s), information system(s), and/or network(s) to allow the threat actor to direct or conduct enabling or malicious activity.
		Manage deployed capability		Steps taken by a threat actor to activate, calibrate, request/status, reconfigure or deactivate deployed Malware, to create conditions that support intended or to initiate malicious activity on victim's computer(s) and/or network(s).
		Establish illicit user access		Activities conducted to gain access to and/or permissions for the intended victim(s)' computer, information systems or data stores, e.g., credential theft, impersonating a known user, spoofing the intended victim into thinking the threat actor is someone else, or by using existing capabilities (i.e., protocol manipulation, application/script/shell exploits, impersonation/spoofing) to authorize account activities for which legitimate access would not normally be granted.

Figure 4. CTF Lexicon Excerpt. Layer 3 Lexicon. Source: ODNI

This is indicative of the power of the Lexicon to accurately convey complex technical concepts to non-technical audiences while supporting the needs of technical analysts.

The Cyber Threat Framework Breaks New Ground

What is fascinating—and disheartening—is that over 95 percent of all incidents investigated recognize "human error" as a contributing factor.

- IBM[13]

Breaking with tradition, the Cyber Threat Framework does not define cyberspace or cybersecurity. By not defining cyberspace or cybersecurity, the ODNI has sidestepped definitional turf wars AND created a nomenclature that provides a common language to describe the adversarial engagement which seeks to compromise data processing systems.

Rather than defining "cybersecurity" or "cyberspace," the Cyber Threat Framework defines cyber threats, how these threats progress over time and the consequences of these threats. The Cyber Threat Framework abstracts cyber threats from particular technologies, focusing on the attacker's methodologies, not specific malware vulnerabilities.[14] The hierarchal structure facilitates the description of cyber threats at different levels of detail within the overarching time context. An analysis of the Business Email Compromise using the Cyber Threat Framework,

Figure 5, demonstrates these concepts.[15]

Stages	Objectives	Actions	Indicators
Preparation	Develop resources & capabilities	Create capabilities	- email accounts - bank accounts
	Acquire victim specific knowledge	Research activities	- Social networking interactions - Visits to victim's website
Engagement	Interact with intended victim	Persuade people to act on threat actor's behalf	Email content
	Deliver malicious capability	Send email	Email content
Presence	Establish controlled access	Establish illicit user access	Email content
Effect/Consequence	Alter system behavior	Change decisions	Authorized user misdirects money

Figure 5. Cyber Threat Framework Analysis of Business Email Compromise

In Figure 5, the Cyber Threat Framework describes a cyber threat which is free of malware, stolen credentials, remote access tools or other abuses of, or defects in, data processing systems. The undesired consequences did not occur in the data processing system. The intact data processing system reached the wrong real-world result. In the Cyber Threat Framework, cyber threats matter because of the effects and consequences, not because of the internal workings of the data processing systems. Malware matters, not because it is malware, but because malware is one of the tools threat actors use to create undesired effects and consequences. The Cyber Threat Framework is concerned with the effects threat actors accomplish through the abuse of data processing systems **and the people who operate them**.

Frequently the threat actor requires the authorized user to undertake one or more authorized actions on behalf of the threat actor. For example, ransomware, the fastest growing cybercrime[16], often requires user interaction (e.g., open an attachment, follow a link, download a file) for success. In 2017, the FBI Director fell prey to a reporter's simulated phishing attack.[17] Similarly, the takedown of the Ukrainian power grid required the authorized user to use authorized system privileges to execute three discrete steps (open email, open attachment, enable scripts) to enable the threat actor's malware.[18] In addition to these direct engagements between threat actor and users (in which the threat actor is communicating with the user), there are indirect engagements between threat actors and users. In these indirect engagements the users know that the proverbial the wolf is at the door, yet the users fail to bar the door, choosing, instead, to engage in insecure behaviors.[19] The Cyber Threat Framework supports robust analysis of the interactions, both direct and indirect, between threat actors and authorized users which interactions are often essential elements in the cyber incidents.

People – The Path Less Travelled by Defenders

The new [US$100 bill] design incorporates security features that make it easier to authenticate, but harder to replicate... [T]he user-friendly security features will allow the public to more easily verify its authenticity.

- Jerome H. Powell, Federal Reserve Board Governor[20]

Threat actors often leverage actions of authorized users to compromise systems. The generally accepted model of user behavior is set forth in the Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.). As we discuss below, the Cyber Threat Framework adopts a more expansive view of human behavior than FISMA. The Cyber Threat Framework's more expansive view of human behavior aligns defensive analysis with the human vulnerabilities upon which threat actors rely.

Traditionally, user behavior is analyzed with the user awareness model. FISMA codifies the awareness model at 44 U.S.C. §3544(b):

> (4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
>
> (A) information security risks associated with their activities; and
>
> (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

FISMA charges the National Institute of Standards and Technology (NIST) to develop information security standards and guidelines for federal information systems. The NIST framework incorporates FISMA's user awareness risk model as PR.AT, Awareness and Security Training.[21] This awareness risk model is used in NIST's comprehensive cyber security guidance, NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[22] NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, sets forth specific guidance on user cyber security training program.[23]

The user awareness model is pervasive in cyber security.[24] The user awareness model assumes that **users are agents of defense**, with users diligently and effectively complying with security measures. In this system, management is responsible to provide adequate training and users are responsible to implement the training. User related incidents are, thus, the result of either of both of:

- inadequate training programs,
  or
- user error, when users fail to apply their training.

The Defense Science Board summarizes the user awareness model:[25]

> Following an initial education period, failures must have consequences to the person exhibiting unacceptable behavior. At a minimum the consequences should include

removal of access to network devices until successful retraining is accomplished. Multiple failures should become grounds for dismissal. An effective training program should contribute to a decrease in the number of cyber security violations.

In 2015, Paul Beckmen, the then CISO of DHS, described his system of continual user training and retraining reinforced with job actions.[26] Admiral Rogers, NSA Director, took this a step further, arguing for court-martial for someone who clicks on a phishing email.[27] The underlying assumption of this system is that awareness, reinforced with retraining, rewards and punishment, leads to desired behaviors and a secure cyber ecosystem.

The Cyber Threat Framework takes a different approach to user behavior. Threat actors realize that no matter how restricted users' rights are, users must have a vestige of data processing rights to do work. These vestigial user rights, no matter how restricted, create the opening for threat actors. The Cyber Threat Framework acknowledges that cyber threats can result from users being persuaded by threat actors to act on behalf of threat actors.[28] In the Cyber Threat Framework, **users are the nascent agents of the threat actors,** waiting to fall victim to psychological manipulation.[29]

The alternative models of user awareness and psychological manipulation result in vastly different defensive strategies. Under the user awareness risk model, when cyber aware users take actions which compromise systems, these errors are the users' fault and the users are subject to remedial actions. Under the psychological manipulation model, when users make an error, the psychological manipulation that led to the error must be understood; that understanding can then be used to develop defenses against the manipulative processes. While training is, no doubt, one strategy to counter psychological manipulation, the Cyber Threat Framework expands the user-facing defensive toolbox to include all aspects of psychological manipulation.

Using information to psychologically manipulate victims to take actions that benefit the threat actor is a deception information operation.[30] In a deception information operation, the threat actor targets the victim's "information processing, perception, judgment, and decision making."[31] The decision-making process takes place in response to the information presented by a data processing endpoint (e.g., computer, tablet, cellphone). Three factors converge when the user is interacting with the endpoint:

- The information transmitted by the threat actor
- The user interface
- The user's mental processes invoked in response to the transmitted information as presented in the user interface.

Each of these three factors contribute to the success of a cyber threat information operation. Threat actors create the material that they transmit taking into account how the user will respond to that information in the context of the interface. The interface itself is subject to a wide array of deceptive practices which are very difficult or impossible for users to detect. Conti and Sobiesk observe:[32]

> Malicious interfaces are extremely prevalent in a variety of contexts and a deeper understanding is required by human computer interaction and security professionals as well as end users in order to counter and mitigate their impact.

The user's mental processes take place in the context of the user's overall operating environment in which users operate data processing systems to accomplish work objectives. To the extent that security tasks are inconsistent with productive tasks, a conflict is created between productive work and security work. Psychologists have established that users manage this conflict with a mental compliance budget.[33] **The Compliance Budget teaches that users continuously weigh the value of security tasks against mission tasks and that users do not implement security tasks which, in the user's view, are too costly.**

In 2017, the FBI Director clicked on a reporter's simulated phishing email.[34] The reporter constructed an email which, when displayed in the Director's interface, appeared to be from a trusted sender. The content of the message was crafted to induce the Director to interact with the email, in this case, an email invitation to view a Google Docs spreadsheet. It was technically feasible to determine that this email was suspicious. Under the user awareness model, interacting with the email was the Director's fault and remedial actions focus on the consequences that should befall him.

Under the psychological manipulation model, the inquiry seeks to understand the psychology of the interaction between the threat actor and the user. The general description of this type of threat actor-user interaction is the victim is an object inspector and the threat actor is exploiting the user's knowledge and authentication processes to deceive the user.[35] Applying the psychological manipulation model to the simulated phishing email which ensnared the FBI Director reveals the complex interaction of the three factors discussed above (transmitted information, user interface, user environment) as the user undertakes the email inspection process. The Director did not undertake a forensic review of the reporter's bogus email because people do not interact with emails in that manner. Instead, users manage their Compliance Budget when processing email by applying a triad of simple rules of thumb driven by perceived relevance, urgency clues and habit.[36] As the Director's actions show, the user interface makes it relatively easy for threat actors to manipulate the email triad to deceive the user into a compromising inspection result. The ease with which email can be used for deception makes email an important tool of threat actors. Jeh Johnson, former DHS Secretary, observed, "The most devastating attacks by the most sophisticated actors very often start because somebody opened an email that they shouldn't open."[37]

The user task of identifying threatening emails is merely one example of the general problem of inspection systems that favor threat actors. For example, in the Ukrainian power grid takedown, the threat actor leveraged several system design deficiencies to deceive the user into performing a carefully orchestrated series of insecure behaviors. The user sequentially inspected the email, the attachment and the attachment's security notice, each time incorrectly concluding that the interaction was safe. At each step along the way, the threat actor manipulated the data processing system to lead the user to the threat actor's desired object inspection result.

Recently discovered flaws in modern CPU's have become an opportunity for threat actors.[38] However, the threat actors are not exploiting the CPU flaws. Instead, threat actors are exploiting the users as object inspectors. The threat actors are sending phishing emails which have links to fake patch URL's. When the users inspect the emails, the content and call-to-action are consistent with the general awareness of the CPU problem and remedies.[39] When the user clicks the link and arrives at the destination URL, again the threat actor forces the user to act as an object inspector. The careful, well-trained cyber-aware user acting as a URL inspector will look for https indicators to support a rigorous authentication process. Anticipating such a user, the threat actor undermines the inspection process by manipulating the authentication process with https indicators. The https indictors of trusted websites and threat actors' websites are indistinguishable to non-expert users. Unremarkably, when the authentication indicators of trusted counterparts and threat actors are indistinguishable, users reach undesired inspection results.

Cyber security is not the only encounter in which non-expert users are exploited as object inspectors. Criminals often cast non-expert users in the role of object inspector. Our daily lives are filled with object inspection decisions which are subject to malicious manipulation. In the spring of 2004, the FBI commenced an investigation into North Korean counterfeit US$100 bills of such superb quality that even Secret Service currency examiners were fooled.[40] The US$100 bill is the most commonly used currency in the world. Everyone is aware of counterfeit currency and nobody wants to receive worthless counterfeit money. Despite the awareness of counterfeit money, the U.S. government did not respond to this problem with a program to train the world's population to be expert currency examiners. Instead, the U.S. Government redesigned the US$100 bill to include user-friendly security features that North Korea could not easily duplicate. This easy-to-authenticate/hard-to-replicate model is not unique to currency. Easy-to-authenticate/hard-to-duplicate is used in a wide variety of situations, such as tamper-evident packaging, in which non-expert users are required to be object inspectors. Effective implementations of easy-to-authenticate/hard-to-duplicate object inspection invoke the psychological suspicion response; suspicion is a psychological process which is distinct from trust and trustworthiness.[41] When design is done correctly, user inspection processes can be improved while simultaneously increasing the obstacles imposed on threat actors.[42]

The problem of poor design is broader than creating opportunities for threat actors to directly manipulate user object inspection. As users go about their daily activities, users' responses to poor design unwittingly create opportunities for threat actors. As users do their jobs, they can degrade security to manage their Compliance Budget. For example, poor password practices make life easier for users while undermining password policies, resulting in easy to compromise credentials.[43] Users create risky Shadow IT systems which are outside of the protections created by information assurance professionals.[44] Users even take measures to circumvent or disable security systems that interfere with job tasks.[45] Failing to perform crucial security tasks such as patch management leave systems vulnerable to known threats.[46] Risky behaviors implemented by users for user convenience create opportunities for threat actors.[47]

Poor usability forces poor compliance which, in turn, creates system vulnerabilities which threat actors exploit.[48] Under the user awareness model, training programs absolve cyber defense

professionals from responsivity for losses attributed to user actions. When trained users make errors, the user is responsible, not the incentives of the operating environmental created by cyber defense professionals. The Cyber Threat Framework requires an inquiry into the psychological factors exploited by threat actors. NIST's Visualization and Usability Group observed:[49]

> **The goal is to build systems that are actually secure not theoretically secure: Security Mechanisms have to be usable in order to be effective.**

The psychology of usability looks at the totality of the man-machine interaction in the context of the user's operating environment.[50] By looking at the psychology of user behavior, the Cyber Threat Framework brings cyber threat analysis in line with the general practice of holding designers responsible for undesired outcomes that result from poor usability.[51] Under the Cyber Threat Framework, security professionals cannot avoid responsibility for poor design by simply blaming the users for the system vulnerabilities caused by deploying poorly designed user environments.[52]

The Cyber Threat Framework Needs Cyber Hygiene.

I don't brief my daughter on streptococcal or meningococcal anything. I said, "Brush your teeth, wash your hands, don't share food." I give her that basic hygiene to successfully get through her day.

- Jane Holl Lute, former Deputy Secretary, Department of Homeland Security[53]

The Lexicon accomplishes its goals of a common language of cyber threats and facilitating information sharing and metrics to evaluate threat activity.[54] However, the Lexicon inadequately addresses the efficacy of cyber defensive measures.

During May 2017 the WannaCry ransomware attack caused system availability problems around the world.[55] Cyber hysteria swept the world, including blaming the U.S. Government.[56] WannaCry was reported as a sophisticated attack which held the world hostage.[57] WannaCry is yet another example of the "Legend of Sophistication in Cyber Operations" in which the failure of cyber defenses is attributed to an adversary with cyber powers beyond our meager defensive resources, requiring a cyber response of increased investment in ever more powerful defensive systems.[58] In reality, WannaCry victims did not require custom defenses driven from real-time detailed cyber-intelligence about specific indicators of compromise. Trend Micro documented how a few simple non-specific defenses could have prevented or mitigated the WannaCry event.[59] The defenses that Trend Micro identified are examples "cyber hygiene." Cyber hygiene consists of general defensive measures which are not in response to specific threat indicators.

In 2015 the NSA released an eight-page cyber-hygiene handbook called, *NSA Methodology for Adversary Obstruction* (MAO).[60] Unlike the frameworks referenced in the Cyber Threat Framework, which characterize the activities of the threat actor, the MAO looks at the actions of target. This target-based approach sets forth the general defensive actions of cyber hygiene.

The MAO can provide the basis of a proposed fifth layer for the Lexicon. We propose that this fifth layer be called "Victimology." Victimology consists of the target's operations security shortcomings which contribute to the Effect/Consequence. The first eleven Layer 2 Objectives

are the NSA's recommended defensive strategies. The last two Layer 2 Objectives are not contained in the MAO. The penultimate Layer 2 Objective defensive strategy, Training and Usability, addresses the risks of users falling victim to psychological manipulation which was identified in the Cyber Threat Framework together with vulnerabilities users introduce in response to poor design. The final defensive strategy, Business Continuity Plans, addresses the failure of targets to mitigate system availability threats attributable to a lack of advanced planning.[61] For the sake of clarity, Layer 4 Indicators and "Definitions" are excluded from Figure 6, Victimology.

Layer 1 Stages	Layer 2 Objectives	Layer 3 Actions
Victimology	The failure of the target to implement non-specific defensive measures that can be taken which are not in response to specific threat indicators.	
	Protect Credentials	
		Implement Least Privilege
		Restrict Local Accounts
		Limit Lateral Movement
		Admin Access Segregation
		Admin Access Protection
		Ensure Administrative Accounts do not have email accounts or Internet access
		Utilize Strong Authentication
		Log and Monitor Privileged Admin Account Usage
		Log and Monitor Use of Administrative Tools
	Segregate Networks and Functions	
		Know your Network
		DMZ Isolation
		Network Function Segregation
		Limit Workstation-to-Workstation Communications
		Perimeter Filtering
		Use Web Domain Name System (DNS) Reputation
		Restrict or Prevent Remote Admin Access
	Implement Host Intrusion Prevention System (HIPS) Rules	
	Centralize logging of all events	
	Take Advantage of Software Improvement	
	Implement Application Whitelisting	
	Install and correctly use EMET	
	Public Services Utilization	
	Use a Standard Baseline	
	Data-at-Rest and Data-in-Transit Encryption	
	Use Anti-Virus File Reputation Services	
	Training and Usability	
	Business Continuity Plans	

Figure 6. Proposed Sixth Stage, Victimology.
Adapted from NSA, Methodology for Adversary Obstruction

The MAO provides detailed definitions of the first eleven Layer 2 Objectives and related Layer 3 Actions. Usability, a term used in the penultimate Action, is defined as, "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."[62] The terms "Training" and "Business Continuity Plans" can be defined by reference to the respective NIST documents.[63]

Conclusion

[W]hat keeps me up at night now is the wide diversity of threats that we have from all across the world, including the ever-expanding list of cyber threats.

- Dan Coats, Director of National Intelligence[64]

The variety of cyber threats facing our nation is vast. As the ODNI observed in publishing the Cyber Threat Framework, understanding these threats has been hampered by the lack of a common language to describe the threats. This lack of understanding is sometimes an intentional strategy which seeks to hide failure behind obfuscating language.[65] The Cyber Threat Framework provides a system of analysis which eschews terms like "hacking," "advanced" and "sophisticated," instead adopting a system which objectively describes the actions of threat actors using a hierarchal stage-driven lexicon. The Lexicon can be used and understood by data processing experts and non-experts to achieve a common understanding. Of particular importance is the Cyber Threat Framework's psychological model of users.

However, the Cyber Threat Framework's focus on the actions of the threat actors leaves potential victims without clear defensive guidance. We have proposed adding a fifth stage, Victimology, to the Cyber Threat Framework. By reporting relevant Victimology in the cyber threat analysis, defenders will be able to see the contribution targets make to their own fate and steps to take to avoid becoming victims themselves.

The views expressed herein are the views of the authors and do not reflect the views of Iconix, Inc. or PepsiCo, Inc.

---

[1] "Cyber Threat Framework." *Office of the Director of National Intelligence*. ODNI, 13 Mar. 2017. Web. 10 Jan.2018. <https://www.odni.gov/index.php/cyber-threat-framework>.
[2] ODNI, Fn. 1
[3] A Common Cyber Threat Framework: A Foundation for Communication." *Office of the Director of National Intelligence*. ODNI, 13 Mar. 2017. Web. 3 Jan. 2018. https://www.odni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf>. Slide 3.
[4] "Cyber Threat Framework: Frequently Asked Questions (FAQ)." *Office of the Director of National Intelligence*. ODNI, 13 Mar. 2017. Web. 10 Jan. 2018. <https://www.odni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_FAQs.pdf>.
[5] ODNI, Fn. 3. Slide 4.
[6] ODNI, Fn. 4.
[7] "Cyber Threat Framework Version 4.0 Lexicon of concepts and definitions." *Office of the Director of National Intelligence*. ODNI, 13 Mar. 2017. Web. 3 Jan. 2018.Page 1.

<https://www.odni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon.pdf>
.
[8] ODNI, Fn. 3. Slide 9.
[9] ODNI, Fn. 7, Page 1.
[10] ODNI, Fn. 3. Slide 10.
[11] ODNI, Fn. 7.
[12] ODNI, Fn. 7. Page 5.
[13] "IBM Security Services 2014 Cyber Security Intelligence Index." *SCMagazine*. IBM, June 2014. Web. 10 Feb. 2018. <https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf>.
[14] Discussing the Ukraine blackout attack, Robert M. Lee, a former cyber warfare operations officer for the US Air Force, observed, "In terms of sophistication, most people always [focus on the] malware [that's used in an attack]. To me what makes sophistication is logistics and planning and operations and ... what's going on during the length of it. And this was highly sophisticated." Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *WIRED*. CNMN Collection, 3 Mar. 2016. Web. 2 Jan. 2018. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
[15] "Business E-Mail Compromise." *News*. FBI, 27 Feb. 2017. Web. 22 Feb. 2018. <https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise>.
[16] Ashford, Warwick. "Ransomware Was Most Popular Cyber Crime Tool in 2017." *ComputerWeekly.com*. TechTarget, 25 Jan. 2018. Web. 1 Feb. 2018. <http://www.computerweekly.com/news/252433761/Ransomware-was-most-popular-cyber-crime-tool-in-2017>.
[17] Feinberg, Ashley, Kashmir Hill, and Surya Muttu. "Here's How Easy It Is to Get Trump Officials to Click on a Fake Link in Email." *GIZMODO*. Gizmodo Media Group, 9 May 2017. Web. 8 Jan. 2018. <https://gizmodo.com/heres-how-easy-it-is-to-get-trump-officials-to-click-on-1794963635>.
[18] Ashford, Fn. 16.
[19] Kirlappos, Iacovos, Adam Beautement, and M. Angela Sasse. ""Comply or Die" Is Dead: Long live security-aware principal agents." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2013.
[20] "Federal Reserve Board Issues Redesigned $100 Note." *Press Release*. Board of Governors of the Federal Reserve System, 8 Oct. 2013. Web. 1 Feb. 2018. <https://www.federalreserve.gov/newsevents/pressreleases/other20131008a.htm>.
[21] Sedgewick, Adam. *Framework for improving critical infrastructure cybersecurity, version 1.0. No. NIST-Cybersecurity Framework.* 2014.
[22] Ross, Ronald S. *Security and Privacy Controls for Federal Information Systems and Organizations [includes updates as of 5/7/13]*. No. Special Publication (NIST SP)-800-53 Rev 4. 2013.
[23] Wilson, Mark, and Joan Hash. "SP 800-50. Building an Information Technology Security Awareness and Training Program." (2003).
[24] Blau, Alex. "Better Cybersecurity Starts with Fixing Your Employees' Bad Habits." *Security and Privacy*. Harvard Business Review, 11 Dec. 2017. Web. 12 Feb. 2018. <https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits>.

Defense Science Board. "Resilient Military Systems and the Advanced Cyber Threat," *Department of Defense*, January 2013, Web March 1, 2013, Defense Science Board.

"Resilient Military Systems and the Advanced Cyber Threat," Department of Defense, January 2013, Web. March 1, 2013.
<http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Dey, Debabrata, Abhijeet Ghoshal, and Atanu Lahiri. "Security Circumvention: To Educate or To Enforce?." *Proceedings of the 51st Hawaii International Conference on System Sciences*. 2018.

[25] Defense Science Board, Fn. 24. Page 69.
[26] Kyzer, Lindy, *Phishing Fools Would Lose Clearance if DISA CISO Gets His Way*, ClearanceJobs.com, 23 September 2015. Web. 15 November 2015, https://news.clearancejobs.com/2015/09/23/phishing-fools-lose-clearance-disa-ciso-gets-way/
Moore, Jack, *If You Fall For A Phishing Scam, Should You You're your Security Clearance?*, Nextgov, 18 September 2015. Web. 21 June 2016, <http://www.nextgov.com/cybersecurity/2015/09/if-you-fall-phishing-scam-should-you-lose-your-security-clearance/121427/>.

[27] Berman, Dennis K, "Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor," *Wall Street Journal*, 26 October 2015. Web. 26 October 2015.
<http://www.wsj.com/article_email/adm-michael-rogers-on-the-prospect-of-a-digital-pearl-harbor-1445911336-lMyQjAxMTA1NzIxNzcyNzcwWj>.
[28] ODNI, Fn. 7. Page 4.
[29] ODNI, Fn. 7. Page 3.
[30] Joint Publication (JP) 3-13, *Information Operations*.
Joint Publication (JP) 3-13.4, *Military Deception*.
[31] JP-3-13. Page I-3
[32] Conti, Gregory and Edward Sobiesk. "Malicious Interface Design: Exploiting the User," *WWW 2010*, April 26–30, 2010, Raleigh, North Carolina, USA.
[33] Beautement, Adam, M. Angela Sasse, and Mike Wonham. "The compliance budget: managing security behaviour in organisations." *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 2009.
[34] Feinberg, Fn. 17.
[35] "The Need for Global Standards and Solutions to Combat Counterfeiting." *White Paper*. GS1, 9 Apr. 2013. Web. 12 Feb. 2018. <https://www.gs1.org/docs/GS1_Anti-Counterfeiting_White_Paper.pdf>.
[36] Vishwanath, Arun, et al. "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model." *Decision Support Systems* 51.3 (2011): 576-586.
[37] "Russian Interference in 2016 Election." *C-SPAN.org*, C-SPAN, 21 June 2017, <www.c-span.org/video/?430063-1/jeh-johnson-russia-orchestrated-election-cyberattacks-change-tally-outcomes&start=3763>. Jeh Johnson at 1:05:30.
[38] Tung, Liam. "Windows Meltdown-Spectre: Watch out for Fake Patches That Spread Malware." *ZDNet*. CBS Interactive, 16 Jan. 2018. Web. 10 Feb. 2018.
<http://www.zdnet.com/article/windows-meltdown-spectre-watch-out-for-fake-patches-that-spread-malware/>.

[39] "Alert (TA18-004A) Meltdown and Spectre Side-Channel Vulnerability Guidance." *US-Cert*. Department of Homeland Security, 4 2018. Web. 1 Feb. 2018. <https://www.us-cert.gov/ncas/alerts/TA18-004A>.
[40] Rose, David. "North Korea's Dollar Store." *Vanity Fair*. Condé Nast, Sept. 2009. Web. 11 Feb. 2018. <https://www.vanityfair.com/style/2009/09/office-39-200909>.
[41] Vishwanath, Arun, Brynne Harrison, and Yu Jie Ng. "Suspicion, cognition, and automaticity model of phishing susceptibility." *Communication Research* (2016): 0093650215627483.
[42] We apply the principles of usability to email to show how the email interface can be modified to improve security and usability. See Zager, John, and Robert Zager. "Improving Cybersecurity Through Human Systems Integration." *Small Wars Journal*. Small Wars Foundation, 22 Aug. 2016. Web. 18 Sept. 2017. <http://smallwarsjournal.com/jrnl/art/improving-cybersecurity-through-human-systems-integration>.
[43] Inglesant, Philip G., and M. Angela Sasse. "The true cost of unusable password policies: password use in the wild." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010.
[44] "1H 2017 Shadow Data Report: Enterprise Cloud Applications & Services Adoption, Use, Content and Threats." *Symantec*. Symantec Corp., 11 Oct. 2017. Web. 23 Feb. 2018. <http://images.mktgassets.symantec.com/Web/Symantec/%7B86cedfbd-899e-47f3-95c6-f500c0a3427f%7D_Symc_IR_CloudSOC_ShadowDataReport-1H2017_En_v7j.pdf>.
[45] Kirlappos, Fn. 19.
[46] Bilge, Leyla, and Tudor Dumitras. "Before we knew it: an empirical study of zero-day attacks in the real world." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012.
[47] Pallas, Frank. "Information Security Inside Organizations-A Positive Model and Some Normative Arguments Based on New Institutional Economics." (2009).
[48] Theofanos, Mary. *Poor Usability: The Inherent Insider Threat*. Gaithersburg, MD: National Institute of Standards and Technology, 2008. *Computer Security Resource Center*. NIST, 21 Mar. 2008. Web. 22 Sept. 2017. <https://csrc.nist.gov/CSRC/media/Presentations/Poor-Usability-The-Inherent-Insider-Threat/images-media/Usability_and_Insider_threat.pdf>.
[49] Theofanos, Fn. 48, Slide 13.
[50] NASA. *Systems Engineering Handbook.* NASA/SP-2007-6015, Rev 1.
[51] Human error is a common problem. For example, in aircraft crash investigations, a finding of pilot error often includes a finding of poor design which led to the human error.

Salmon, Paul M., Guy H. Walker, and Neville A. Stanton. "Pilot error versus sociotechnical systems failure: a distributed situation awareness analysis of Air France 447." *Theoretical Issues in Ergonomics Science* 17.1 (2016): 64-79.

Colombia. Aeronautica Civil. *AA965 Cali Accident Report Near Buga, Colombia, Dec 20, 1995*. By Rodrigo C. Cabrera, Orlando R. Jimenez, and Saul G. Pertuz. Bogata, Colombia, September 1996. Networks and Distributed Systems. University of Bielefeld - Faculty of Technology, 6 Nov. 1996. Web. 3 Jan. 2018. <http://sunnyday.mit.edu/accidents/calirep.html>.

United States. National Transportation Safety Board. *Descent Below Visual Glidepath and Impact With Seawall Asiana Airlines Flight 214 Boeing 777-200ER, HL7742 San Francisco, California July 6, 2013*. Washington, D.C: National Transportation Safety Board, June 24, 2014.

Aircraft pilots are not the only people who make errors as the result of poor design. Between 1990 and 2003, 42% of construction fatalities were related to design issues. United States. Occupational Safety and Health Administration. *Design for Construction Safety*. Department of Labor, June 24, 2015.

Automobile design can contribute to driver errors. Kieler, Ashlee. "More Than 100 Crashes Caused By Confusing Jeep, Chrysler, Dodge Gear Shifters." *Consumerist*. Consumer Media LLC, a Not-for-profit Subsidiary of Consumer Reports, 8 Feb. 2016. Web. 4 Jan. 2018. <https://consumerist.com/2016/02/08/more-than-100-crashes-caused-by-confusing-jeep-chrysler-dodge-gear-shifters/>.

[52] The law of product liability, which shifts losses from users to designers, is founded on the premise that designers are responsible for the undesired outcomes of their designs. See Restatement (Third) Torts: Products Liability (1998).

[53] "The Darkening Web." *C-SPAN.org*, C-SPAN, 17 July 2017, <https://www.c-span.org/video/?431356-2/the-darkening-web&start=3226>. Jane Holl Lute at 53:49.

[54] "The Merits of Adopting a Common Approach to Describing and Measuring Cyber Threat." *Office of the Director of National Intelligence*. ODNI, 13 Mar. 2017. Web. 10 Jan. 2018. <https://www.odni.gov/files/ODNI/documents/features/A_Common_Threat_Framework_Food_for_Thought.pdf>.

[55] "WannaCry Ransomware Attack." *Wikipedia*. Wikimedia Foundation, Inc., 17 Feb. 2018. Web. 23 Feb. 2018. <https://en.wikipedia.org/wiki/WannaCry_ransomware_attack>.

[56] O'Brien, Chris. "Microsoft President Blasts NSA for Its Role in 'WannaCry' Computer Ransom Attack." *Los Angeles Times*. Los Angeles Time, 14 May 2017. Web. 23 Feb. 2018. <http://www.latimes.com/world/europe/la-fg-europe-computer-virus-20170514-story.html>.

[57] Fox-Brewster, Thomas. "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak." *Security*. Forbes, 17 May 2017. Web. 1 Feb. 2018. <https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#45d56241e599>.

[58] Buchanan, Ben. *The Legend of Sophistication in Cyber Operations*. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2017.

[59] "WannaCry/Wcry Ransomware: How to Defend against It." *Security News*. Trend Micro Incorporated, 13 May 2017. Web. 1 Feb. 2018. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it>.

[60] "NSA Methodology for Adversary Obstruction." *Information Assurance Directorate*. NSA/IAD, 15 Sept. 2015. Web. 26 Jan. 2017. <https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/reports/assets/public/upload/NSA-Methodology-for-Adversary-Obstruction.pdf&WpKes=aF6woL7fQp3dJizXCkcbwTeLkU9HubDMyr393t>.

[61] Bartock, Michael. *SP 800-184 Guide for Cybersecurity Event Recovery. NIST-Cybersecurity Framework.* 2014.

[62] ISO 9241-11

[63] Wilson, Fn. 23.
Bartock, Fn. 61.

[64] Coats, Dan. "Remarks as Delivered by the Honorable Dan Coats Director of National Intelligence – Billington Cybersecurity Summit." *Speeches & Interviews 2017*. Office of the Director of National Intelligence, 9 2017. Web. 1 Feb. 2018.

<https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2017/item/1797-remarks-as-delivered-by-the-honorable-dan-coats-director-of-national-intelligence-billington-cybersecurity-summit>.
[65] Buchanan, Fn. 58.