Cyber Threat Characterization

Dr. Kamal T. Jabbour
Dr. Erich Devendorf

ABSTRACT

In this article, we discuss the threat component of the risk to information systems. We review traditional cyber threat models, then present a technical characterization of the cyber threat along ten dimensions. We cross-reference an industry analysis of the Stuxnet threat to illustrate our thinking and conclude with an outline of the threat model application to the development of Cyber Red Books™.

1. INTRODUCTION

In prior work on cyber risk assessment[1], we referred to the National Institute of Standards (NIST) decomposition of risk into its three constituents of vulnerability, threat, and impact[2] as the guiding principle for cyber vulnerability assessment. Focusing primarily on developing a repeatable methodology for vulnerability assessment, answering the "what" question of risk, we introduced a characterization of the threat along ten dimensions, from education and training, to resourcing and access.

In this article, we expand our characterization of the threat along these ten dimensions and seek to answer the "how" question of risk. We draw on the analysis of Stuxnet for clarifying distinctions and supporting arguments.

We start the article by reviewing de facto threat models used across the industry and identifying their limitations, and we conclude by outlining the potential application of the threat model to the development of a Cyber Red Book™ to guide security professionals in prioritizing their investments in vulnerability mitigation and mission assurance.

2. TRADITIONAL THREAT MODELS

The cyber risk to an information system is a function of (1) the likelihood of a potential vulnerability, (2) the possibility of a threat exploiting the vulnerability, and (3) the impact of successful exploitation. The potential vulnerability and the impact

Dr. Kamal T. Jabbour, a member of the scientific and technical cadre of senior executives, is Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry.

constitute the "what" component of the risk equation, while the threat addresses the "how" question.

A viable cyber threat requires three components:

- Capability: the talent, time, and treasure to create an adverse impact against a target;
- Access: remote or physical access to the target system, or access-less, and
- Intent: which we assume is present.

As we discuss commonly-used models of cyber threat, we caution against the dangers of mirror-imaging–the mistake of attributing to the adversary our way of thinking and our way of fighting. In this historical era of conflict that spans the entire gamut from asymmetric warfare to peer nation-state skirmishes, we cannot afford to dismiss doctrines, cultures or values that differ from ours.

2.1 CYBER THREAT TRENDS

In a 2001 Statement for the Record for the Joint Economic Committee on Cyber Threat Trends and US Network Security [3], Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, talked about the following potential cyber threats and actors that can challenge the US:

- National Government threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption.
- Terrorists are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries.
- Industrial Spies and Organized Crime Groups pose a medium-level threat to the US through their ability to conduct industrial espionage

Dr. Erich Devendorf is the Director of the Advanced Course in Engineering and Air Force Research Laboratory Early Career Award recipient. As a Computer Engineer at the Air Force Research Laboratory Information Directorate, Dr. Devendorf addresses enduring Air Force challenges at the boundaries between Air, Space and Cyberspace. His assurance work represents a shift away from homogeneous systems to heterogeneous entities designed to complete the mission. He is an internationally recognized creator of multinational, joint training exercises that leverage cross domain fires and multi-domain operations.

and large-scale monetary theft as well as their ability to hire or develop hacker talent.

- Hacktivists pose a medium-level threat of carrying out an isolated but damaging attack; most international hacktivist groups appear bent on propaganda.
- Hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures.

Gershwin recognized that globally available tools in 2001 were effective against general-purpose Internet targets, but that specialized tools were needed against hard targets. He also recognized that the skills necessary to develop and employ advanced tools remained a limiting factor for many adversaries.

2.2 GAO THREAT TABLE

In 2005, the Government Accountability Office (GAO) presented a cyber threat table in a report on the role of the Department of Homeland Security in cyber security for critical infrastructure protection [4]. The threat table included an expanded list of threat actors and their tradecraft:

- Bot-network operators are hackers who take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks.
- Criminal groups seek to attack systems for monetary gain, commit identity theft and online fraud. International corporate spies and organized crime also pose a threat to the US through industrial espionage, large-scale monetary theft and their ability to hire/develop hacker talent.

- Foreign intelligence services use cyber tools in information-gathering and espionage. Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities to enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power.
- Hackers break into networks for the thrill of the challenge or for bragging rights. While attack tools have become more sophisticated, they have also become easier to use. The large majority of hackers do not have the requisite expertise to threaten critical U.S. networks, but the worldwide population of hackers poses a relatively high threat of an isolated disruption causing serious damage.
- Disgruntled organization insiders remain a principal source of computer crime. The insider threat also includes outsourcing vendors, as well as, employees who accidentally introduce malware into systems.
- Phishers execute phishing schemes in an attempt to steal identities or information for monetary gain. May use spam and spyware/malware to accomplish their objectives.
- Spammers distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations.
- Spyware/malware authors carry out attacks against users by producing and distributing spyware and malware.
- Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence.

The GAO table recognizes implicitly the wide range of talent, time, and treasure necessary for each threat category to achieve its objective, with a commensurate range of potential consequences.

3. THE TEN DIMENSIONS OF THE CYBER THREAT

A science and technology examination of recent malicious cyber activity led to the formulation of the following ten-dimensional model to characterize a nation state threat.

3.1 HIGHLY EDUCATED ON THE SCIENCE OF INFORMATION ASSURANCE

Bloom's Taxonomy of Learning[5] defines six major cognitive categories, ranging from knowledge, comprehension and application, to analysis, synthesis and evaluation. We categorize the lower three cognitive categories under the broad umbrella of training and consider the upper three categories as the foundations of education.

In a 2008 open letter to US universities[6], Mary Ann Davidson lamented the lack of a secure development lifecycle in the vast majority of degree programs. Davidson called for a revolution in software engineering education, starting with integrating security into the fabric of every course so that engineers can build systems that are safe, secure, and reliable.

In 2011, the White House[7] added its voice to the chorus calling for scientific rigor in cybersecurity and called for the development of an organized, cohesive scientific foundation that promotes the discovery of laws, hypothesis testing, and capabilities to design and evolve high-assurance systems whose assurance properties can be verified.

While the calls for scientific rigor remain unheeded in US cyber workforce development, evidence points to the opposite in peer nations. Recent results of the annual International Collegiate Programming Contest[8] reveal the domination by teams from Russia and China, accounting for ten times more top ten teams than US universities. It goes beyond conjecture to conclude that these graduates, highly educated on the science of information assurance, contribute to the cyber capabilities of their nations.

3.2 DOCTRINALLY TRAINED ON THE ART OF CYBER WARFARE

A Preliminary Assessment of National Doctrine and Organization for Cybersecurity and Cyberwarfare[9] identified 33 states that included cyberwarfare in their military planning and organization. The role of cyber in military doctrine ranged from surveillance and reconnaissance, to information operations against critical targets.

The 1999 thought piece “Unrestricted Warfare”[10] outlined how two Chinese People’s Liberation (PLA) Army colonels viewed the role of information warfare in compensating for the asymmetrical US advantage in kinetic capabilities. The authors called for unrestricted warfare using all military means against a superior adversary, and provided a doctrinal road map to train Chinese cyber warriors. A 2004 White Paper on National Defense increased the PLA focus on “informationalization” and advocated the use of cyber and electronic warfare in the early stages of a conflict.

In 2010, the Russian Federation discussed the characteristics of modern military conflict in an updated military doctrine that called for the early use of information warfare to achieve military objectives without the use of military force. The 2016 iteration on the Russian doctrine appears defensive in nature, and it focuses on strategic deterrence and prevention of conflicts that might result from information warfare. The Russian doctrine[11] calls for training cyber warriors by conducting more exercises and practice scenarios of large cyberattacks against multiple targets.

3.3 ADEQUATELY RESOURCED IN TALENT, TIME, AND TREASURE

Contrary to urban legends that portray cyber actors as anti-social teenage prodigies who live in basements and subsist on pizza and soda, the nation state cyber threat enjoys an abundance of talent, time, and treasure. The mathematical foundations of information theory, signals communications, and encryption necessitate advanced education in these subjects as minimum entry requirements into the field of cyber warfare. The dominant culture of engineering and mathematics in Russia and China, and the large number of universities that deliver the requisite formal education result in a large pool of available talent to fuel cyber warfare.

Besides talent, it takes time to analyze complex missions and systems, map their dependence on cyberspace, and identify potential cyber vulnerabilities. The development of offensive cyber agents that can exploit such vulnerabilities to generate adverse effects requires additional time, and the test and validation of the resulting weapons require even more time. The cycle of mission analysis, cyber dependence, agent development, and test and validation may take several months to a few years.

We estimate treasure in terms of the cost in personnel and materiel resources necessary for the effective generation of cyber effects against a target. We define the cost of personnel in terms of talent and time. Materiel resources include hardware and software computing resources, communication systems for the delivery, and command and control of the cyber agent. Access to a connected target through remote means, or to a stand-alone target by bridging the air gap, also contribute to the necessary treasure.

3.4 THOROUGHLY BRIEFED ON TARGET MISSIONS AND SYSTEMS

Few cyber phenomena have captured the fascination of the media and the general public more than information theft through cyber exploitation and data exfiltration. From the theft of millions of background investigation records from the computers of the Office of Personnel Management [12] to the widely-publicized theft of US military aircraft trade secrets [13], a growing body of evidence suggests that near-peer adversaries have acquired detailed knowledge of the design and function of US weapons and systems. Therefore, rather than assume security through obscurity when it comes to hiding the dependence on cyber of critical missions, we must accept as a starting position that nation adversaries are thoroughly briefed on US targets and missions.

Military intelligence points to similarities between foreign and US aircraft as evidence of cyber exploitation of trade secrets from major defense contractors. The recent showcase of the Chinese J-20 stealth fighter revealed numerous similarities to the US F-22 Raptor, leading officials to accuse China of building its aircraft based on stolen designs of the US aircraft. [14]

Design documentation that permitted an adversary to build a replica of a US weapon may also provide the knowledge necessary to identify and avoid replicating potential cyber vulnerabilities of that weapon. We posit that two possible explanations exist for subtle differences between an original weapon and its replica: (1) a failure to replicate advanced materials and technology, or (2) a deliberate effort to mitigate vulnerabilities in the original weapon.

3.5 MATHEMATICALLY SPECIALIZED IN ARCHITECTURAL PROPERTIES

Architecture encompasses the art and science of design and construction. In cyberspace, architecture refers to the configuration of components and systems that generate, process, store, transmit, consume, and destroy information. Sharing processors, buses, or memory resources creates architectural vulnerabilities that permit the propagation of effects among the processes sharing that resource. For example, an electric short-circuit in one module may trip a circuit-breaker and disconnect other modules, or a system babbling on a bus may prevent other systems from communicating on that bus.

The architectural attribute of resource sharing extends beyond the hardware, software, and networks that compose a system, and includes the users, operators and administrators, as well as, the protocols and policies that govern their roles in the architecture. A formal representation of these relationships provides a mathematical model of potential cyber vulnerabilities and informs threat actors on the ways and means to exploit these vulnerabilities.

A 2010 JASON summer study [15] concluded that cyber security required an understanding of computer science concepts like model checking, cryptography, type theory, and game theory. These mathematical concepts led to a rigorous framework for examining security, developing a specification, and validating assertions about its correctness under specific assumptions, thereby allowing effective reasoning about program security, obfuscation, and prioritization.

3.6 SUPERIORLY SKILLED IN BYZANTINE FAILURE ANALYSIS

The Byzantine Generals Problem [16] refers to an encamped army using messengers to communicate among its generals, where one or more generals could be potential traitors. The solution of the problem requires the loyalty of at least two-thirds of the generals to win the battle. In other terms, each traitor can mislead and confuse at most two loyal generals.

Byzantine failure (or fault) analysis in a distributed information system borrows from the Byzantine Generals Problem and reduces the problem of risk assessment to one of vulnerability-consequence assessment regardless of cause. The focus of Byzantine failure analysis turns away from system reliability “when a computer dies”, to system security, “when a computer lies”. In information assurance terms, a Byzantine failure transforms the input vector from compromise in information availability to compromise of information integrity.

A skillful Byzantine failure analysis of a target system provides an adversary with a new attack dimension that seeks to exploit the implicit trust among system components to generate Byzantine behaviors, and consequently adverse effects.

3.7 INTRICATELY INVOLVED IN PROTOCOL SPECIFICATION AND ANALYSIS

Communication protocols serve a valuable function of allowing compatibility and interconnectivity among disparate implementations by different manufacturers. At the foundation of layered communication protocols lies the provision to permit a Layer N+1 implementation to recover from a failure at Layer N. Each protocol layer offers services to the layer above it and receives service from the layer(s) below it. Incorrect specification of protocols [17] creates potential vulnerabilities independent of specific implementations.

The ubiquitous adoption of commercial protocol standards for military applications brings the benefits of independence from proprietary protocols, compatibility with a broad range of components, and a perception of lower development costs. However, a commercial protocol intended for reliable operation in a permissive environment may exhibit undesirable behaviors in contested operations. In addition, the international organizations that specify, design, and establish protocol standards target their products at common commercial users, without consideration to the risk calculus of military and national security applications.

An undesirable side effect of the globalization of communication protocols may occur as a result of deliberate trade-offs among privacy, reliability, safety, cost, performance, and security. The lack of thorough understanding of the subtle differences among these requirements may result in the hasty adoption of a protocol as a standard without due diligence to mission assurance implications.

3.8 CRITICALLY EMBEDDED IN THE SUPPLY CHAIN

The Department of Defense (DoD) relies on a large number of contractors in the global supply chain, both to build original weapons and to sustain them throughout the decades-long acquisition lifecycle. In a report to Congress, the GAO deemed the DoD supply chain vulnerable to the risk of counterfeit parts, with a potential to disrupt missions and endanger service members. [18]

While the GAO report did not discuss or infer any malicious manipulation of components through either hardware Trojans or backdoors, the potential adverse mission impact of counterfeit parts is likely independent of intent. As we discussed earlier under Byzantine failures, a bad chip–intentional or accidental–carries the potential of adverse mission effect.

The off-shore outsourcing of electronic manufacturing of integrated circuits and computers brings a unique security challenge at the lowest protocol layer, the physical or hardware layer. Similarly, the off-shore outsourcing of software development of operating systems and tools introduces Byzantine uncertainty at the remaining protocol layers, from the firmware layer all the way to the application layer.

3.9 STRATEGICALLY POSTURED IN COMMAND AND CONTROL

A 2015 GAO Report on Defense Satellite Communications[19] recognized that the DoD leased commercial SATCOM to support critical mission needs, from command and control of Unmanned Aerial Vehicles (UAV) to intelligence and communications, costing over $1 billion in 2011. The DoD relies equally on commercial land lines and submarine cables, making a substantial portion of military command and control vulnerable to third-party disruption.

In addition, the GAO quantified further DoD reliance on commercial critical infrastructure in a 2009 report[20] that referred to the 34 most critical assets whose "incapacitation, exploitation, or destruction could severely affect DOD's ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions."

Those critical dependencies on commercial assets render DoD missions vulnerable to threats that could exploit those assets, and expand uncontrollably the scope and range of mission assurance.

3.10 CONVENIENTLY SITUATED FOR ACCESS AND PERSISTENCE

The tyranny of distance characterizes the challenge of fighting a far-off war, even in these days of global connectivity and global mobility. A side effect of fighting abroad is that the adversary enjoys convenient access to resources–spectral, spatial, and temporal. This location convenience translates readily into access and persistence, at times and in places, where the US may find it necessary to establish and re-establish access repeatedly.

4. STUXNET: A COMPLEX THREAT

In this section, we consider Stuxnet in the context of the ten dimensions of the cyber threat, described in Section 3. We chose Stuxnet as an example for three reasons: (1) Experts characterize Stuxnet as the "... first cyber weapon in the world"[21], (2) Major computer security firms studied, analyzed and reported on Stuxnet and (3) Stuxnet is a sophisticated and targeted weapon. The creator of Stuxnet unequivocally exhibits five of the ten dimensions of the cyber threat. They may possess the other five dimensions, but the data available from Stuxnet does not support that conclusion. Before discussing how the characteristics of Stuxnet map to the capability of its creator, we provide a brief timeline from the initial deployment of Stuxnet until the first speculation of its true purpose.

In June 2009, the first variant of Stuxnet began infecting information systems associated with the Iranian nuclear enrichment program. In January 2010, the International Atomic Energy Agency noticed that Iran was replacing centrifuges at their Natanz nuclear enrichment facility at a very high rate[22]. Six months later in June 2010, fully patched Windows computers at Natanz began to blue screen and restart. The antivirus software VirusBlokAda identified the cause of these computer problems as a Windows rootkit, first named Rootkit.Tmphider but popularized as W32.Stuxnet[23]. It was not until 14 July 2010 that Frank Boldewin suggested "… this malware was made for espionage," on the Wilder Security forum [24].

4.1 DOCTRINALLY TRAINED ON THE ART OF CYBER WARFARE

The Natanz enrichment facility is a strategically important center of gravity to the Iranian nuclear program [22]. The International Atomic Energy Agency estimates the nuclear breakout time, defined as the amount of time to manufacture enough high-quality fissile material to produce one nuclear warhead, for a fully functional Natanz facility at 3-6 months [25]. The critical vulnerability of the facility is the need for contractors to regularly install and replace centrifuges at the site.

Given this vulnerability, the actor that created Stuxnet had a well-scoped and targeted mission that attacked the critical vulnerability for this center of gravity. The Stuxnet payload activates in the presence of specific targets, discussed in Section 4.3 and has natural limitations to stop its spread. Analysis has argued that the creators of Stuxnet took pains to remain compliant with the Laws of Armed Conflict (LOAC) [26]. The precision and sophistication of Stuxnet coupled with its LOAC compliance demonstrate that its creator was well versed in the art of cyberwarfare.

4.2 ADEQUATELY RESOURCED IN TALENT, TIME, AND TREASURE

The development of Stuxnet extended far beyond the creation of the software used to exploit the target information systems. Before the creation of the core Stuxnet code, engineers had to design a payload to reliably destroy IR-1 centrifuges [27]. Engineers knowledgeable in machine design and failure analysis designed, developed and tested this payload prior to its employment. Testing requires a significant resource investment to gather the intelligence required to replicate the target system, understand the safeguards in place and construct a representative testbed. With a viable payload, developers created one of the first programmable logic controller rootkits to execute their attack method while simultaneously concealing the attack to avoid detection.

With a viable payload, Symantec estimates the code to deliver that payload to the PLC required a team of five to ten developers working full time for six months [28]. Other reports suggest that as many as three independent teams worked on Stuxnet to integrate and build its individual modules [20]. That development included extensive research to evade ten commercial antivirus products and customized memory injection code. In addition to this, Stuxnet utilized four zero day Windows exploits and two certificates stolen from Realtek and JMicron Technology Corps. Collectively, the scope of Stuxnet suggests an actor with adequate resources in time, talent, and treasure.

4.3 THOROUGHLY BRIEFED ON THEIR TARGET MISSIONS AND SYSTEMS

Stuxnet has a well-defined mission set with safeguards in place to minimize and prevent significant spread beyond its intended target. Stuxnet only infects 32-bit systems in the Windows family from Win 2k through Windows Server 2008 R2. It spreads via USB exploits and over a local area network. These design choices indicate knowledge of both the concept of operations used by its target and the types of systems in use by that target.

Stuxnet uses finer granularity when deploying its payload. The payload only activates when the host system contains the WinCC/Step 7 control software, and it only corrupts the controller when it identifies two specific frequency controllers identified by 7050h and 9500h data blocks [26]. The actor creating Stuxnet possessed the necessary intelligence to craft and deliver a targeted attack that limits collateral damage while still accomplishing its mission.

4.4 SUPERIORLY SKILLED IN BYZANTINE FAILURE ANALYSIS

Although Stuxnet generated destructive effects against IR-1 centrifuges, security professionals did not discover it until it began to blue screen and reboot Windows systems [25]. Stuxnet both covered its tracks and generated an effect that was identical to a typical failure mode of a faulty IR-1. The general unreliability of the IR-1 further obfuscated the presence of Stuxnet.

As a Byzantine failure, Stuxnet replicated a failure in the sensors that measure IR-1 performance. This failure resulted in the operator receiving data that made the centrifuge appear to operate normally when it was, in fact, operating outside its design parameters with all safety features removed. The design flaw that enabled this byzantine failure to generate destructive effects is the collocating of the sensor and control feeds for an IR-1.

4.5 CONVENIENTLY SITUATED FOR ACCESS AND PERSISTENCE

Stuxnet's creators deployed it in three distinct waves [26] starting in 2009 and targeted five distinct contractors that supported the Natanz enrichment facility [25]. The smallest time elapsed from the Stuxnet compilation to the callback in the first Stuxnet wave was twelve hours [26]. This short time suggests convenient access to the target. The presence of multiple Stuxnet waves indicates that access to the initial targets persisted for at least a year from June 2009 through April 2010.

The dimensions we identified in our consideration of Stuxnet's creators demonstrate how to evaluate a threat in the context of capability. In addition to these five factors, an argument can be made that its creators were also embedded in the supply chain, had a mathematical understanding of architectural properties and were well versed in protocol specification and analysis. We restricted our analysis to the clearest cut dimensions. In the next section, we discuss the concept of a Cyber Red Book™ that identifies specific capabilities requires to exploit a system.

5. THE CYBER RED BOOK™

In the Spring 2016 issue of *The Cyber Defense Review,* we introduced the Cyber Blue Book™ as a process to codify cyber vulnerability assessment of information systems, to answer in essence the "what" question in cyber risk assessment. We outlined the following ten steps for developing a Cyber Blue Book™:

1. Identify the mission of the System Under Test (SUT).
2. List Mission Essential Functions (MEF).
3. Map cyber dependence of each MEF across the six phases of the information lifecycle.
4. Draw an information boundary for the SUT.
5. Enumerate the Information Exchange Requirements (IER) between the SUT and the outside world.
6. Characterize each information flow across the information boundary.
7. Estimate mission impact of information flow compromise using Byzantine fault analysis.
8. Characterize impact as disruption, degradation, denial, destruction or deception.
9. Categorize vulnerability in terms of architecture, specification or implementation.
10. Design tests to verify the impact of information flow compromise.

The Cyber Red Book™ seeks to characterize the threats necessary to exploit the potential vulnerabilities that the Cyber Blue Book™ identifies. To that effect, Byzantine failure gives way to malicious conduct, and the focus of the inquiry shifts from answering the "what" to the "how".

In the 2016 paper, we enumerated the information exchanges of a remotely-piloted helicopter, shown in Figure 1, and estimated the adverse effect of a Byzantine corruption to the integrity of the information. Cyber threat characterization requires estimating the threat necessary to compromise the integrity of each information exchange regarding both threat capability and threat access.

For this example, a Cyber Red Book™ examines necessary capability and access:

- GPS spoofing: signal power, angle and location
- 3G/4G interference: power and range to jam or hijack
- Camera and LASER ranging: wavelengths, angle of attack and range

- WiFi: based on security protocol, processing power to break encryption and range
- USB: means to compromise host computer using USB to communicate to the aircraft

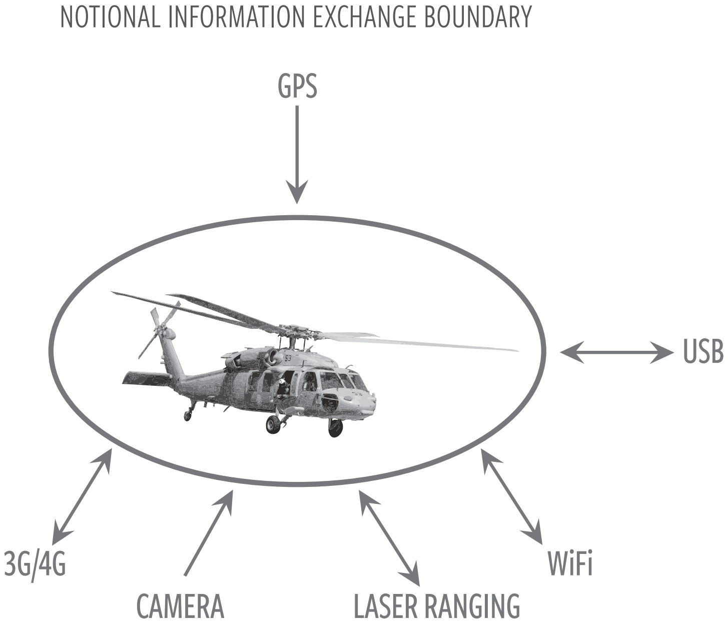

Figure 1. Information Exchange Boundary for RC Helicopter

The Cyber Red Book™ identifies the necessary capabilities to transform a Cyber Blue Book™ failure into a deliberate effect. For the example in Figure 1, at least three dimensions are required to implement a GPS spoof: (1) Conveniently situated for access and persistence, (2) Intricately involved in protocol specification and analysis, and (3) Mathematically specialized in architectural properties.

The nature of the GPS system, low power with line of sight requirements, means an actor must be in close physical proximity to execute a GPS spoof, captured in the first dimension. Effectively spoofing the correct set of GPS packets at the correct power levels to generate an effect requires a strong understanding of the GPS protocol, captured in the second dimension. Finally, an actor must have a strong understanding of the interaction between GPS and the other on-board navigation systems to generate an effect against the platform. That actor requires an even stronger understanding of these interactions to generate the desired effect. In addition to technology driven constraints, the system concept of operations may require an actor to fulfill additional dimensions to reliably generate their desired effect. The dimensions of a cyber threat provide a set of enduring properties for a Cyber Red Book™ that characterizes risk regarding fundamental actor properties.

6. CONCLUSION

In this article, we discussed the threat component of the risk to information systems. We reviewed traditional cyber threat models, then presented a technical characterization of the cyber threat along ten dimensions. We cross-referenced an industry analysis of the Stuxnet threat to illustrate our thinking and concluded by outlining the application of the threat model to the development of Cyber Red Books™.

NOTES

1. Kamal Jabbour and Jenny Poisson, “Cyber Risk Assessment in Distributed Information Systems,” *The Cyber Defense Review,* Spring 2016, 79-100.

2. Guide for Conducting Risk Assessments: Information Security, National Institute of Standards and Technology, NIST Special Publication 800–30-rev1, September 2012.

3. Lawrence K. Gershwin, Statement for the Record for the Joint Economic Committee on Cyber Threat Trends and US Network Security, June 21, 2001.

4. Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).

5. B.S. Bloom et al, “Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain”, New York: David McKay Co Inc., 1956.

6. Mary Ann Davidson, “The Supply Chain Problem”, Oracle Chief Security Officer Blog, April 7, 2008.

7. “Trustworthy Cyberspace”, Strategic Plan for the Federal Cyber Security Research and Development Program, Executive Office of the President, National Science and Technology Council, December 2011.

8. International Collegiate Programming Contest, Baylor University, 2002-2016.

9. James A. Lewis and Katrina Timlin, Cyber Security and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization”, Center for Strategic and International Studies, 2011.

10. Qiao Liang and Wang Xiangsui, “Unrestricted Warfare”, Beijing: PLA Literature and Arts Publishing House, February 1999.

11. Information Security Doctrine of the Russian Federation, 2016.

12. Cyber Incidents, Cyber Security Resource Center, Office of Personnel Management, June 2015.

13. Sydney J. Freedburg Jr., “Top Official Admits F-35 Stealth Fighter Secrets Stolen,” Breaking Defense, June 20, 2013.

14. Alex Lockie, “How China's stealthy new J-20 fighter jet compares to the US's F-22 and F-35,” Business Insider, November 1, 2016.

15. JASON Summer Study, “The Science of Cyber Security”, 2010.

16. Leslie Lamport et al, “The Byzantine Generals Problem,” ACM Transactions on Programming Languages and Systems, Vol 4, No. 3, July 1982, 382-401.

17. Milica Barjaktarovic, Shiu-Kai Chin and Kamal Jabbour, “Formal Specification and Verification of Communication Protocols Using Automated Tools”, First International Conference on Engineering Complex Computer Systems, ICECCS'95, Fort Lauderdale, FL, November 6-10, 1995.

18. United States Government Accountability Office, “COUNTERFEIT PARTS: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,” GAO-16-236, February 2016.

19. United States Government Accountability Office, “DEFENSE SATELLITE COMMUNICATIONS: DOD Needs Additional Information to Improve Procurements,” GAO-15-459, July 2015.

20. United States Government Accountability Office, “DEFENSE CRITICAL INFRASTRUCTURE: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets,” GAO-10-147, October 2009.

21. Sharma, A.R., “Stuxnet-First Cyber Weapon of the World”, Symantec, 21 January 2012.

22. Zetter, K., “Countdown to Zero Day”, Crown, United States, 2014.

23. T.S., “The Stuxnet Worm a Cyber-missile aimed at Iran?”, *The Economist,* September 2010.

24. Boldewin, F., https://www.wilderssecurity.com/threads/rootkit-tmphider.276994/#post-1712134

25. Heinonen, O., “Iran’s Nuclear Breakout Time: A Fact Sheet”, POLICYWATCH 2394, The Washington Institute, March 2015.

26. Foltz, A., “Stuxnet, Schmitt Analysis and the Cyber ‘Use of Force’ Debate”, *Joint Force Quarterly,* 67(4), 2012.

27. Langer, R., “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve”, The Langer Group, November 2013.

28. Falliere,N., Murchu, L., Chien, E., “W32.Stuxnet Dossier,” Symantec Security Response, February 2011.