Cybersecurity Service Model

Harry Katzan, Jr., Webster University, USA

ABSTRACT

The efficacy of modern computer systems is normally regarded as a function of five basic attributes of computer and information security: availability, accuracy, authenticity, confidentiality, and integrity. The concepts generally apply to government, business, education, and the ordinary lives of private individuals. The considerations normally involve extended applications of the Internet – hence the name Cybersecurity. Achieving and maintaining a secure cyberspace is a complicated process, and some of the concerns involve personal identity, privacy and intellectual property, secure maintenance of the critical infrastructure, and the sustainability of organizations. The threats to a secure operating infrastructure are serious and profound: cyber terrorism, cyber war, cyber espionage, and cyber crime, to which the technical community has responded with a plethora of ad hoc safeguards and procedures, usually supplied by the competitive private sector. This paper proposes a fresh view of the cyber domain based on service science with the ultimate objective of developing a cybersecurity service model.

Keywords: Cybersecurity; Information Assurance; Critical Infrastructure Protection; Service Science

INTRODUCTION

The Internet is the newest form of communication between organizations and people in modern society. Everyday commerce depends on it, and individuals use it for social interactions, as well as for reference and learning. To some, the Internet is a convenience for shopping, information retrieval, and entertainment. To others, such as large organizations, the Internet makes expansion cost effective and allows disparate groups to profitably work together through reduced communication costs. It gives government entities facilities for providing convenient service to constituents. The Internet is also efficient, because it usually can provide total service on a large variety of subjects in a few seconds, as compared to a much longer time for the same results that would have been required in earlier times. [11]

From a security perspective, the use of the term "cyber" generally means more than just the Internet, and usually refers to the use of electronics to communicate between entities. The subject of cyber includes the Internet as the major data transportation element, but can also include wireless, fixed hard wires, and electromagnetic transference via satellites and other devices. Cyber elements incorporate networks, electrical and mechanical devices, individual computers, and a variety of smart devices, such as phones, tablets, pads, and electronic game and entertainment systems. A reasonable definition would be that cyber is the seamless fabric of the modern information technology infrastructure that enables organizations and private citizens to sustain most aspects of modern everyday life.

Cyber supports the commercial, educational, governmental, and critical national infrastructure. Cyber facilities are pervasive and extend beyond national borders. As such, individuals, organizations, and nation-states can use cyber for productive and also destructive purposes. A single individual or a small group can use cyber for commercial gain or surreptitious invasion of assets. Activities in the latter category are usually classed as penetration and include attempts designed to compromise systems that contain vital information. In a similar vein, intrusion can also effect the operation of critical resources, such as private utility companies.

Interconnectivity between elements is desirable and usually cost effective, so that a wide variety of dependencies have evolved, and cyber intrusions have emerged. Thus, a small group of individuals can compromise a large organization or facility, which is commonly known as an *asymmetric* threat against which methodological

protection is necessary. In many cases, a single computer with software obtained over the Internet can do untold damage to a business, utility, governmental structure, or personal information. Willful invasion of the property of other entities is illegal, regardless of the purpose or intent. However, the openness of the Internet often makes it difficult to identify and apprehend cyber criminals.

CYBERSECURITY OPERATIONS

It is well established that cybersecurity is a complicated and complex subject encompassing computer security, information assurance, comprehensive infrastructure protection, commercial integrity, and ubiquitous personal interactions. Most people look at the subject from a personal perspective. Is my computer and information secure from outside interference? Is the operation of my online business vulnerable to outside threats? Will I get the item I ordered? Are my utilities safe from international intrusion? Have I done enough to protect my personal privacy? Are my bank accounts and credit cards safe? How do we protect our websites and online information systems from hackers? Can my identity be stolen? The list of everyday concerns that people have over the modern system of communication could go on and on. Clearly, concerned citizens and organizations look to someone or something else, such as their Internet service provider or their company or the government, to solve the problem and just tell them what to do.

So far, it hasn't been that simple and probably never will be. The digital infrastructure based on the Internet that we call cyberspace is something that we depend on every day for a prosperous economy, a strong military, and an enlightened lifestyle. Cyberspace, as a concept, is a virtual world synthesized from computer hardware and software, desktops and laptops, tablets and cell phones, and broadband and wireless signals that power our schools, businesses, hospitals, government, utilities, and personal lives through a sophisticated set of communication systems, available worldwide. However, the power to build also provides the power to disrupt and destroy. Many persons associate cybersecurity with cyber crime, since it costs persons, commercial organizations, and governments more than a $1 trillion per year.[1] However, there is considerably more to cybersecurity than cyber crime, so it is necessary to start off with a few concepts and definitions.

Cyberspace has been defined as the interdependent network of information technology infrastructure, and includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries.[2] Alternately, cyberspace is often regarded as any process, program, or protocol relating to the use of the Internet for data processing transmission or use in telecommunication. As such, cyberspace is instrumental in sustaining the everyday activities of millions of people and thousands of organizations worldwide.

CYBER ATTACKS

Cyber attacks can be divided into four distinct groups:[3] cyber terrorism, cyber war, cyber crime, and cyber espionage. It would seem that cyber crime and cyber espionage are the most pressing issues, but the others are just offstage. Here are some definitions:[4]

- *Cyber crime* is the use of computers or related systems to steal or compromise confidential information for criminal purposes, most often for financial gain.
- *Cyber espionage* is the use of computers or related systems to collect intelligence or enable certain operations, whether in cyberspace or the real world.
- *Cyber terrorism* is the use of computers or related systems to create fear or panic in a society and may result in physical destruction by cyber agitation.

[1] Remarks by the U.S. President on Securing Our Nation's Cyber Infrastructure, East Room, May 29, 2009. [1]
[2] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). [2]
[3] Shackelford, Scott L., In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012, Stanford Law Review, March 8, 2012, http://www.stanfordlawreview.org [20]
[4] Lord, K.M. and T. Sharp (editors), America's Cyber Future: Security and Prosperity in the Information Age (Volume I), Center for New American Security (June 2011), http://www.cnas.org [16]

- *Cyber war* consists of military operations conducted within cyberspace to deny an adversary, whether a state or non-state actor, the effective use of information systems and weapons, or systems controlled by information technology, in order to achieve a political end.

As such, cybersecurity has been identified as one of the most serious economic and national security challenges facing the nation.[5] There is also a personal component to cybersecurity. The necessity of having to protect one's identity and private information from outside intrusion is a nuisance resulting in the use of costly and inconvenient safeguards.

CYBERSPACE DOMAIN, ITS ELEMENTS AND ACTORS

Cyberspace is a unique domain that is operationally distinct from the other domains of land, sea, air, and space. It provides, through the Internet, the capability to create, transmit, manipulate, and use digital information.[6] The digital information includes data, voice, video, and graphics transmitted over wired and wireless facilities between a wide range of devices that include computers, tablets, smart phones, and control systems. The Internet serves as the transport mechanism for cyberspace. The extensive variety of content is attractive to hackers, criminal elements, and nation states with the objective of disrupting commercial, military, and social activities. Table 1 gives a list of areas at risk in the cyberspace domain.[7] Many cyber events, classified as cyber attacks, are not deliberate and result from everyday mistakes and poor training. Others result from disgruntled employees. Unfortunately, security metrics include non-serious as well as serious intrusions, so that the cybersecurity threat appears to be overstated in some instances. This phenomenon requires that we concentrate on deliberate software attacks and how they are in fact related, since the object is to develop a conceptual model of the relationship between security countermeasures and vulnerabilities.

Table 1. Areas at Risk in the Cyberspace Domain

Commerce
Industry
Trade
Finance
Security
Intellectual property
Technology
Culture
Policy
Diplomacy

Many of the software threats can be perpetrated by individuals or small groups against major organizations and nation-states – referred to as *asymmetric attacks.* The threats are reasonably well known and are summarized in Table 2. It's clear that effective countermeasures are both technical and procedural, in some instances, and must be linked to hardware and software resources on the defensive side. The security risks that involve computers and auxiliary equipment target low-end firmware or embedded software, such as BIOS, USB devices, cell phones and tablets, and removable and network storage. Operating system risks encompass service packs, hotfixes, patches, and various configuration elements. Established counter measures, include intrusion detection and handling systems, hardware and software firewalls, and antivirus and anti-spam software.

[5] National Security Council, The Comprehensive National Cybersecurity Initiative, The White House, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative [2]

[6] McConnell, M., *Cyber Insecurities: The 21st Century Threatscape,* Chapter II in Lord, K.M. and T. Sharp (editors), America's Cyber Future: Security and Prosperity in the Information Age (Volume II), Center for New American Security (June 2011), http://www.cnas.org [18]

[7] Stewart, J., *CompTIA Security+ Review Guide,* Indianapolis: Wiley Publishing, Inc., 2009. [21]

Table 2. Security Threats

Privilege escalation
Virus
Worm
Trojan horse
Spyware
Spam
Hoax
Adware
Rootkit
Botnet
Logic bomb

The cybersecurity network infrastructure involves unique security threats and countermeasures. Most of the threats relate to the use of out-of-date network protocols, specific hacker techniques, such as packet sniffing, spoofing, phishing and spear phishing, man-in-the-middle attacks, denial-of-service procedures, and exploiting vulnerabilities related to domain name systems. Countermeasures include hardware, software, and protective procedures of various kinds. Hardware, software, and organizational resources customarily execute the security measures. There is much more to security threats and countermeasures, and the information presented here gives only a flavor to the subject.

There is an additional category of threats and countermeasures that primarily involves end-users and what they are permitted to do. In order for a threat agent to infiltrate a system, three elements are required: network presence, access control, and authorization. This subject is normally covered as the major features of information assurance and refers to the process of "getting on the system," such as the Internet or a local-area network. A threat agent cannot address a system if the computer is not turned on or a network presence is not possible. Once an end user is connected to the computer system or network, then access control and authorization take over. It has been estimated that 80% of security violations originate at the end-user level.[8] *Access control* concerns the identification of the entity requesting accessibility and whether that entity is permitted to use the system. *Authorization* refers to precisely what that entity is permitted to do, once permitted access. There is a high-degree of specificity to access-control and authorization procedures. For example, access control can be based on something the requestor knows or what it is. Similarly, authorization can be based on role, group membership, level in the organization, and so forth. Clearly, this category reflects considerations which the organizations has control over, and as such, constitutes security measures that are self-postulated.

The above information constitutes a synopsis of cybersecurity necessary for this paper. Cybersecurity, as an academic discipline, is considerably more extensive.

NAÏVE SERVICE SCIENCE

It is well established that a *service* is a provider/client interaction that creates and captures value. Both parties participate in the transaction, and in the process, both benefit from it. In a sense, the provider and client co-produce the service event, because one can't do without the other. [15] Another view of service is that it is the deployment of service assets by a set of service participants for the benefit of another set of service participants, defined here as economic entities including individuals, businesses, educational institutions, and government agencies and are generally classed as providers and clients when a service event is instantiated. In fact, some economists have classed most products as service providers, since they provide tangible or intangible benefit to a service entity. [12, 19, 22]

Informational systems that are used by people, such as computer systems and the Internet, are also classed as services. In fact, the phenomena of users interacting with computer-based service systems that rely on other computers, as in web services, are also classed as services. In general, the role of service provider and a service client are *complementary*, since one cannot do without the other, and this concept is known as *service duality*. [14]

[8] Stewart, ***op cit***.

When two entities work together to achieve a common purpose, on the other hand, their form of behavior is regarded as *supplementary*. [13]

Normally, systems that provide services exhibit a lifecycle consisting of the following layers of activity: commitment, production, availability, delivery, analysis, and termination. Many societal systems reflect a lifecycle, and that group includes facilities for cybersecurity and information assurance. [13]

SERVICE COLLECTIVISM

Most services operate in a well-defined area of endeavor, such as a university, newspaper, or a medical group. In an operational domain of this sort, there exists a set of providers, a set of clients, and a set of available services. In a colloquial sense, an element of the provider set interacts with an element of the client set instantiating a service from the service set; the interaction creates a service event. [14] The connection between the provider and client sets is viewed as a mapping between the sets in the same sense that a function is a mapping between the domain and co-domain in mathematics. A common means of representing this mapping can be denoted by:

S: *P* -> *C*

where the service (**S**) assigns to each provider *p* in ***P*** an element *c* in ***C***. Clearly, ***P*** refers to the set of providers and ***C*** refers to the client set. The concept is slightly more complicated. Take a university as an example. The set of services provided to students is commonly partitioned as administrative services, academic services, and student services, where the last group addresses the wide variety of personal concerns normally related to students. The service providers in each category commonly coordinate amongst themselves as well as between categories. Some students require multiple services while others need few, if any. An analogous case is a newspaper where readers chose between sections of interest.

Two considerations are of particular interest. The first, and perhaps most important, is the salient fact that service providers in the categories of ***P*** collaborate between themselves and with service providers in other sections. Thus, the set ***P*** is a *service collective.* Later, we are going to reflect on the possibility of elements in ***P*** performing service on elements of themselves.

The second consideration serves to initiate the notion of *service duality*. In the mapping of an element of ***P*** with an element of ***C***, mathematical function theory serves as a useful model. Three forms are identified: surjection, injection, and bijection. With surjection, every element in ***C*** is a service interaction for at least one provider in ***P***. Thus, every element of ***C*** is covered. With injection, every element in ***C*** is a service interaction for most one provider in ***P***. The relationship is a bijection if it is a surjection and an injection for all elements in ***P*** and ***C***. Thus, the phenomena that a provider gives service to multiple clients, i.e., injection, is true only if a temporal form is established.

The key point concerning service duality is that if there is no need for a particular form of service within a given domain, then the necessity of related activity is diminished. If a service provider doesn't have any clients, is it really a service provider or does it exist in some intermediate form. Economic considerations would certainly apply to this situation, so then the question is "To what types of service does this form of analysis apply?"

COLLABORATION SERVICE

A *collaboration service* exists when a total provider set ***P*** supplies a totality of services for a specific domain to a complete client set ***C***. Not every provider p_i performs the same service but the members of ***P*** can collectively supply all of the service needed for that domain. If a product-as-a-service is incorporated in that domain, then it is incorporated in that collaboration group. If a form of service included procedures that must be performed by the client to achieve a service, then that process is additionally included in the collaboration group. Similarly, if certain conditions, or state of the system, must exist within the client area in order for a particular service event to be accomplished, then those *a priori* conditions should be part of the collaboration group. Thus, a

collection of potential provider services, products, processes, and conditions is regarded as a *collaboration group* that provides service to clients in a complex operational domain.

CYBERSECURITY COLLABORATION GROUP

The controls that constitute a cyber security domain form a collaboration group. Diverse elements of hardware and software are used for network and operating system security. Processes are necessary for gaining network presence, access control, and authentication. Intrusion detection and prevention systems (IPDS) are implemented to perform continuous monitoring and cyber protection. Access roles and operational rules are developed to facilitate use of cyber security procedures and elements. Clearly, cybersecurity is a service, albeit a special kind of service in which the distinction between providers and clients is more often blurred rather than being strictly defined.

When a client adopts cybersecurity principles for network presence, access control, and authentication, for example, it applies the inherent methods for and by itself, thereby assuming the dual role of provider and client. Similarly, when an organization installs a hardware or software firewall for network protection, it is effectively applying a product for its own security.

In a service system, service entities exchange information and behavior in order to achieve mutually beneficial results. As service systems become more complex, the service entities adapt to optimize their behavior – a process often referred to as *evolution*. [17] Differing forms of organization emerge such that the system exhibits intelligent behavior based on information interchange and the following nine properties: emergence, co-evolution, sub-optimal, requisite variety, connectivity, simple rules, self organization, edge of chaos, and nestability. Systems of this type are usually known as *complex adaptive systems*. [12] Complex adaptive systems are often known as "smart systems," and cybersecurity researchers are looking at the operation of such systems as a model for the design of cybersecurity systems that can prevent attacks through the exchange of information between security elements.

DISTRIBUTED SECURITY

The major characteristic of a cybersecurity system designed to prevent and mediate a cyber attack is that the totality of security elements in a particular domain are organized into a smart service system. This characteristic refers to the facility of cyber elements to communicate on a real-time basis in response to cyber threats. Currently, threat determination is largely manual and human-oriented. An intrusion detection system recognizes an intrusion and informs a security manager. That manager then contacts other managers via email, personal contact, or telephone to warn of the cyber threat. In a smart cybersecurity system, the intrusion detection software would isolate the cyber threat and automatically contact other elements in the domain to defend their system. Thus, the security service would handle intruders in a manner similar to the way biological systems handle analogous invasions: recognize the threat; attempt to neutralize it; and alert other similar elements.

In a definitive white paper on distributed security, McConnell [18] recognizes the need for cyber devices to work together in near real-time to minimize cyber attacks and defend against them. This is a form of continuous monitoring and referred to as a *cyber ecosystem* in which relevant participants interact to provide security and maintain a persistent state of security. Clearly, a cyber ecosystem would establish a basis for cybersecurity through individually designed hierarchies of security elements, referred to as security devices. Ostensibly, security devices would be programmed to communicate in the event of a cyber attack. The conceptual building blocks of an ecosystem are automation, interoperability, and authentication. *Automation* refers to the notion of security devices being able to detect intrusion detection and respond to other security devices without human intervention. Thus, the security ecosystem could behave as a security service and provide speed and in the activation of automated prevention systems. *Interoperability* refers to the ability of the cyber ecosystem to incorporate differing assessments, hardware facilities, and organizations with strategically distinct policy structures. *Authentication* refers to the capability to extend the ecosystem across differing network technologies, devices, organizations, and participants.

Thus, the cyber ecosystem responds as a service system in requests for security service to participants that are members of the ecosystem, namely private firms, non-profit organizations, governments, individuals, processes, cyber devices comprised of computers, software, and communications equipment.

MONROE DOCTRINE FOR CYBERSECURITY

Internet governance refers to an attempt at the global level to legislate operations in cyberspace taking into consideration the economic, cultural, developmental, legal, political, and cultural interests of its stakeholders. [9] A more specific definition would be the development and application by governments and the private sector of shared principles, norms, rules, decision-making, and programs that determine the evolution and use of the Internet. [9] Internet governance is a difficult process because it encompasses web sites, Internet service providers, and hackers and activists and involves differing forms of content and operational intent ranging from pornography to terrorist information to intrusion and malicious content. Cybersecurity is a complex form of service that purports to protect against intrusion, invasion, and other forms of cyber terrorism, crime, espionage, and war. But, attacks can be carried out by anyone with an Internet connection and a little bit of knowledge of hacking techniques. NATO has addressed the subject of cyber defense with articles that state the members will consult together in the event of cyber attacks but are not duty bound to render aid. [8] It would seem that deterrence, where one party is able to suggest to an adversary that it is capable and willing to use appropriate offensive measures, is perhaps a useful adjunct to cybersecurity service. However, successful attribution of cyber attacks is not a fail proof endeavor so that offensive behavior is not a total solution.

Cybersecurity is a pervasive problem that deserves different approaches. Davidson [10] has noted an interesting possibility, based on the volume of recent cyber attacks. The context is that we are in a cyber war and a war is not won on defense. A "Monroe Doctrine in Cyberspace" is proposed, similar to the Monroe Doctrine of 1823 that "here is our turf; stay out or face the consequences."

SUMMARY

The Internet is a seamless means of communication between organizations and people in modern society; it supports an infrastructure that permits cost effective commerce, social interaction, reference, and learning. The use of the term "cyber" means more than just the Internet and refers to the use of electronics in a wide variety of forms between entities. Cyber facilities are pervasive and extend beyond national borders and can be used by individuals, organizations, and nation states for productive and destructive purposes. A single individual or small group can use cyber technology for surreptitious invasion of assets to obtain vital information or to cause the disruption of critical resources.

Cybersecurity is conceptualized as a unique kind of service in which providers and clients collaborate to supply service through shared responsibility, referred to as *collaborative service*. Cybersecurity is achieved through distributed security implemented as a smart service system with three important attributes: automation, interoperability, and authentication. A Monroe Doctrine for Cybersecurity is proposed.

ACKNOWLEDGMENT

Thanks to Margaret Katzan for reading the manuscript.

AUTHOR INFORMATION

Professor Harry Katzan, Jr. is the author of books and papers on computer science, service science, and security. He teaches cybersecurity in the graduate program at Webster University. E-mail: katzanh@hargray.com

REFERENCES

1. Cavelty, M., Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture, *IP – Global Edition*, ETH Zurich, 3/2011.
2. Conway, M., Terrorism and Internet Governance: Core Issues, Dublin: *Disarmament Forum 3*, 2007.
3. Davidson, M., *The Monroe Doctrine in Cyberspace*, Testimony given to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Technology, March 10, 2009.
4. Katzan, H., Essentials of Cybersecurity, Southeastern INFORMS Conference, Myrtle Beach, SC, October 4-5, 2012.
5. Katzan, H., *Foundations of Service Science: A Pragmatic Approach*, New York: iUniverse, Inc., 2008.
6. Katzan, H., Service Analysis and Design, International Applied Business Research Conference, Orlando, FL, January 4-6, 2010.
7. Katzan, H., Service Collectivism, Collaboration, and Duality Theory, International Applied Business Research Conference, Orlando, FL, January 4-6, 2010.
8. Katzan, H., *Service Science: Concepts, Technology, Management*, New York: iUniverse, Inc., 2008.
9. Lord, K.M. and T. Sharp (editors), *America's Cyber Future: Security and Prosperity in the Information Age* (Volume I), Center for New American Security (June 2011), http://www.cnas.org
10. Mainzer, K., *Thinking in Complexity: The Complex Dynamics of Matter, Mind, and Mankind*, New York: Springer, 1997.
11. McConnell, B. (co-author) and The Department of Homeland Security, Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf, 23 March 2011.
12. National Security Council, *The Comprehensive National Cybersecurity Initiative*, The White House, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
13. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).
14. Norman, D., *Living with Complexity*, Cambridge: The MIT Press, 2011.
15. Remarks by the U.S. President on Securing Our Nation's Cyber Infrastructure, East Room, May 29, 2009.
16. Shackelford, Scott L., In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012, *Stanford Law Review*, March 8, 2012, http://www.stanfordlawreview.org
17. Stewart, J., *CompTIA Security+ Review Guide*, Indianapolis: Wiley Publishing, Inc., 2009.
18. The Department of Homeland Security, *More About the Office of Infrastructure Protection*, http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm
19. The Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*, 2009.
20. The White House, *The National Strategy to Secure Cyberspace*, February 2003.
21. Vargo, S. and M. Akaka, Service-Dominant Logic as a Foundation for Service Science: Clarification, *Service Science* 1(1): 32-41, 2009.
22. Working Group on Internet Governance, Report Document WSIS-II/PC-3/DOC/5-E, August 2005.