ESSENTIALS OF CYBERSECURITY

Harry Katzan, Jr., Webster University, USA

ABSTRACT

The ongoing effectiveness and efficiency of modern networked computer systems is a function of five basic attributes: availability, accuracy, authenticity, confidentiality, and integrity. The concepts apply to information, computers, networks, and other elements of coordination, cooperation, and control, and they apply to government, business, education, and private individuals. The concerns normally involve the Internet as a communication facility – hence the name *Cybersecurity*. The purpose of this paper is to give a composite picture of what cybersecurity is all about, identify the important literature on the subject, and describe how it differs from everyday information security affecting individuals and computer activities.

INTRODUCTION

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? 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 concepts and definitions.

CONCEPTS AND DEFINITIONS

Cyberspace has been defined as the interdependent network of information technology infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[2] Alternately, cyberspace is often regarded as any process, program, or

[1] Remarks by the U.S. President on Securing Our Nation's Cyber Infrastructure, East Room, May 29, 2009.

[2] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

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.

The strategic plan for the U.S. Department of Homeland Security lists five main missions for the period 2012-2016, listed as follows:[3]

Mission 1: Preventing Terrorism and Enhancing Security
Mission 2: Securing and Managing Our Borders
Mission 3: Enforcing and Administering Our Immigration Laws
Mission 4: Safeguarding and Securing Cyberspace
Mission 5: Ensuring Resilience to Disaster

Clearly, the placement of cybersecurity as one of the five major strategic missions of the Department of Homeland Security (DHS) is a sure-fire indication that an underlying problem exists with the global dependence on the Internet that is summarized in the following introductory quote from the DHS report:[4]

> Cyberspace is highly dynamic and the risks posed by malicious cyber activity often transcend sector and international boundaries. Today's threats to cybersecurity require the engagement of the entire society – from government and law enforcement to the private sector and most importantly, members of the public – to mitigate malicious activities while bolstering defensive capabilities.

Ensuing policy goals and objectives to achieve cybersecurity could therefore include:

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment

Objective 4.1.1: Understand and prioritize cyber threats
Objective 4.1.2: Manage risks to cyberspace
Objective 4.1.3: Prevent cyber crime and other malicious uses of cyberspace
Objective 4.1.4: Develop a robust public-private cyber incident response capability

Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Objective 4.2.1: Enhance public awareness
Objective 4.2.2: Foster a dynamic workforce
Objective 4.2.3: Invest in innovative technologies, techniques, and procedures

While the line between policy and operations may be a blurred line in some instances, a necessary requirement of cybersecurity is to have security operations be part of a stated set of objectives.

CYBER ATTACKS

Cyber attacks can be divided into four distinct groups:[5] cyber terrorism, cyber war, cybercrime, and cyber espionage. It would seem that cybercrime and cyber espionage are the most pressing issues, but the others are just offstage. Here are some definitions:[6]

[3] http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf.

[4] Ibid. p.12.

[5] 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).

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 not result in physical destruction by cyber agitation.

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.[7]

THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE

In order to achieve cybersecurity, from individual, national, organizational, or global perspectives, a proposed set of major goals has been developed:[8]

To establish a front line of defense against today's immediate threats
To defend against the full spectrum of threats
To strengthen the future cybersecurity environment

Starting from the top, the President has directed the release of a summary description of the Comprehensive National Cybersecurity Initiatives, summarized as follows:

Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.

Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.

Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.

Initiative #4. Coordinate and redirect research and development (R&D) efforts.

Initiative #5. Connect current cyber ops centers to enhance situational awareness.

Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan.

Initiative #7. Increase the security of our classified networks.

Initiative #8. Expand cyber education.

Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs.

---

[6] 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).

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

[8] Ibid., p.1.

Initiative #10. Define and develop enduring deterrence strategies and programs.

Initiative #11. Develop a multi-pronged approach for global supply chain risk management.

Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

The basic idea of the twelve initiatives is to address current and future cybersecurity issues by combining the resources of the Federal government, local and state governments, and the private sector to provide a strong response to future cyber incidents and by strengthening public/private relationships.

CRITICAL INFRASTRUCTURE AND KEY RESOURCES

The present concern over cybersecurity is the result of a variety of cyber attacks, intrusions, and countermeasures that have occurred globally in recent years. The threat scenarios are multidimensional and attribution is cumbersome to ascertain. Moreover, exposure to cyber threats can be direct or indirect, resulting from a dependence on one or more elements of critical infrastructure. The scope of inherent infrastructure has grown from ten in the year 2003[9] to eighteen in the year 2012.[10] The underlying philosophy is that once the critical areas are identified, a public/private dialog can be established to achieve a measurable amount of cybersecurity. Each of the six critical areas are classed as major and are assigned a Sector Specific Agency (SSA) by the Department of Homeland Security as part of the National Infrastructure Protection Plan (NIPP), intended to set national priorities, goals, and requirements for effective allocation of resources.[11] The major areas are:

Chemical
Commercial Facilities
Critical Manufacturing
Dams
Emergency Services
Nuclear Reactors, Materials, and Waste

The manner in which the public/private coordination and collaboration is executed is a matter of public debate. The key point is that a cyber intrusion in a major area can indirectly endanger a large number of people, governmental organizations, and commercial facilities.

The remaining twelve critical areas are assigned to existing governmental offices, as reflected in the following list:

Agriculture and food – Department of Agriculture and the Food and Drug Administration
Banking and Finance – Department of the Treasury
Communications – Department of Homeland Security
Defense Industrial Base – Department of Defense
Energy – Department of Energy
Governmental Facilities – Department of Homeland Security
Information Technology – Department of Homeland Security
National Monuments and Icons – Department of the Interior
Postal and Shipping – Transportation Security Administration

---

[9] The White House, *The National Strategy to Secure Cyberspace,* February, 2003, p. xiii.

[10] Homeland Security, *More About the Office of Infrastructure Protection,* p. 1, (http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm).

[11] Ibid., p.1.

Healthcare and Public Health – Department of Health and Human Services
Transportation Systems – Transportation Security Administration and the U.S. Coast Guard
Water – Environmental Protection Agency

National and global protection necessarily involves the establishment of a framework to provide the following:[12]

The exchange of ideas, approachs, and best practices
The facilitation of security planning and resource allocation
The establishment of structure for effective coordination among partners
The enhancement of coordination with the international community
The building of public awareness

The identification of the areas of critical infrastructure is significant because of the wide diversity of cyber threats, vulnerabilities, risk, and problem domains. Moreover, critical elements possess a wide variety of technological attributes that require a range of solutions.

SUMMARY

The paper gives an overview of the emerging discipline of cybersecurity that adds a policy level to the longstanding subjects of information security, computer security, and network security. Concepts and some basic definitions are covered. Cyber attacks are divided into cyber crime, cyber espionage, cyber terrorism, and cyber war. A comprehensive overview of the subject matter is given through the National Cybersecurity Initiative, and the notion of the critical infrastructure is explored in some detail.

REFERENCES

Remarks by the U.S. President on Securing Our Nation's Cyber Infrastructure, East Room, May 29, 2009.

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

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).

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).

National Security Council, *The Comprehensive National Cybersecurity Initiative*, The White House, (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative).

The White House, *The National Strategy to Secure Cyberspace*, February, 2003.

Homeland Security, *More About the Office of Infrastructure Protection*, (http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm).

The Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*, 2009.

[12] The Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*, 2009, p. 13.

AUTHOR INFORMATION

Professor Harry Katzan, Jr. is the author of books and papers on computer science, decision science, and service science. He teaches cybersecurity in the graduate program at Webster University.