

Crosscutting Issues in International Transformation

Interactions and Innovations
among People, Organizations,
Processes, and Technology

Edited by Derrick Neal, Henrik Friman,
Ralph Doughty, and Linton Wells II



THE CENTER FOR TECHNOLOGY AND
NATIONAL SECURITY POLICY
NATIONAL DEFENSE UNIVERSITY
WASHINGTON, DC

December 2009

The views expressed in these essays are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources were drawn from unclassified materials.

Portions of this book may be quoted or reprinted without permission, provided that a standard source credit line is included.

This book was published by the Center for Technology and National Security Policy, National Defense University, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at www.ndu.edu/ctnsp/publications.html.

Essay 11

What do Senior Leaders Need to Know About Cyberspace?

By Jeffrey Caton

Abstract

Cyberspace can be an enabler for beneficial transformation, but it also can be exploited as a dark force to thwart such efforts. International entities cannot extract themselves from cyberspace. What must senior security leaders know about cyberspace to transform their organizations and make wise decisions? How does the enduring cyberspace process interact with and transform organizations, technology, and people, and, in turn, how do they transform cyberspace itself?

To evaluate these questions, this essay establishes the enduring nature of the cyberspace process and compares this relative constant to transformation of organizations and people. Each section discussing these areas provides an assessment of their status as well as identifies key issues for senior security leaders to comprehend now and work to resolve in the future. Specific issues include viewing cyberspace as a new strategic common akin to the sea, comparing effectiveness of existing hierarchies in achieving cybersecurity against networked adversaries, and balancing efficiency and effectiveness of security against the universal laws of privacy and human rights. Finally, leaders need to scan the strategic horizon for potential cyberspace-related technological and societal trends and shocks and provide clear visions for success to their organizations.

Introduction

The growth of worldwide cyberspace-related capabilities is a double-edged sword. Cyberspace can be used as an enabler for beneficial transformation, but it also can be exploited as a dark

force to thwart such efforts.¹ Senior security leaders must deal with both sides, and with increasing frequency and greater risks to their missions. Simply put, international entities cannot extract themselves from cyberspace. Given this, what must senior security leaders know about cyberspace to transform their organizations and make wise decisions? How does the enduring cyberspace process interact with and transform organizations, technology, and people, and in turn, how do they transform cyberspace itself?

This essay addresses broad applications of the cyberspace process across diplomatic, informational, military, and economic communities worldwide. Although it discusses technological implications, it avoids detailed technical aspects that might detract from the strategic nature of the content.

To evaluate the central questions posed here, this essay establishes the enduring nature of the cyberspace process and compares this relative constant to transformation of organizations and people. Of course, none of these dimensions exist in isolation—the analytical simplification of evaluating one variable at a time enhances focus and readability. Each section provides an assessment of the status of the dimensions and identifies key issues for senior security leaders to comprehend now and work to resolve in the future.

Background

The term *cyberspace*² often carries an aura of mystery that may belie its fundamental nature. Many respected authors assert that cyberspace and its applications are revolutionary. Rather than argue this point, I posit that the basic process governing cyberspace is defined

¹ The following definitions are used for this chapter: *Cyberspace* is (1) a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (England 2008) and their operators; (2) a new strategic common, analogous to the sea as an international domain of trade and communication (Cebrowski 2004). *Transformation* is a process that shapes the changing nature of competition and cooperation through new combinations of concepts, capabilities, people, and organizations (Rumsfeld 2003, 3)

² Science fiction author William F. Gibson is credited with coining the term “cyberspace” and popularizing it in his book *Neuromancer* (Gibson 1984)

easily. Further, when viewed as a “strategic common,” cyberspace indeed shares many characteristics with the sea, but it also has unique ones as well (Cebrowski, 2004). These distinctive aspects relevant to security within cyberspace are the focus of this essay.

In its simplest form, the cyberspace process consists of three elements—cognitive, informational, and physical (Woolley, 2006). For example, someone generates and articulates a thought (cognitive), and enters the thought into a communication device (physical), where it becomes a systematic representation of data (information), possibly represented digitally using electromagnetic means. Next, the data travels through a variety of physical lines of communication (e.g., telephone, cable, fiber optic line, radio, microwave, etc.), where it exits through a communication device to another user for cognitive use, or perhaps to a physical device to perform an operation (e.g., turn on a light, open a valve).

What is cyberspace, then? It is the sum total of all elements required for cyberspace processes to occur. The fundamental structure of the cyberspace process is enduring, but the configuration of cyberspace itself transforms when specific elements of the basic process transform. This is an essential concept for the analysis of cyberspace transformation addressed in this essay.

To illustrate this further, let us consider the evolution of the cyberspace process since the invention of electromagnetic transmission. As depicted in figure 1, the telegraph is an early example of the cyberspace process. An operator would read a message and enter it as data (Morse code) using a simple switch that sent pulses of electric current to a remote receiving switch, where a different operator would decode the taps into the original message. This basic process evolved in scope and complexity for over 100 years. In the mid-twentieth century, the process was transformed with the introduction of electronic transistor-based data-processing devices.

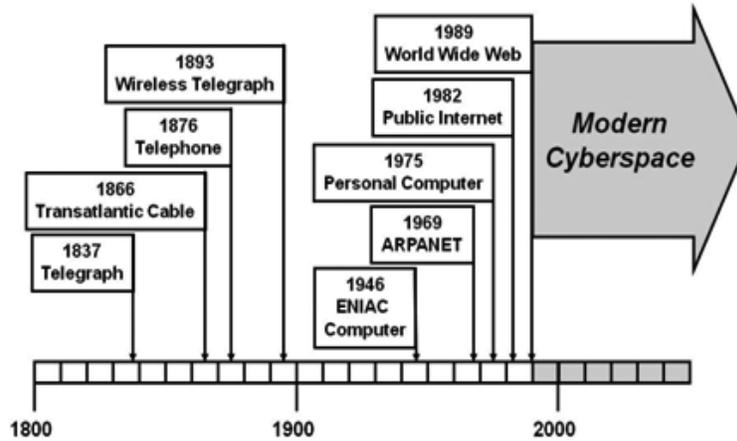


Figure 1: A Brief Timeline of Cyberspace Development

I posit that although the cyberspace process has existed for centuries, cyberspace as currently envisioned came into existence with the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the World Wide Web protocol (circa 1989). The synergy of these events established cyberspace as a new strategic common analogous to Mahan’s theories in which the sea is described as “a wide common” that was the international domain of commerce and communication (Cebrowski, 2004). Similarly, cyberspace can be mapped using techniques that clearly show its lines of communication and critical nodes with tactical, operational, and strategic implications for their control.³ The Cooperative Association for Internet Data Analysis in San Diego, California, is pioneering the macroscopic measurement and analysis of Internet performance, developing several practical maps of topology, security, routing, and other aspects (Claffy et al., 2008). When combined with innovative graphical depictions, these maps clearly show nodes and choke points—the cyberspace equivalent of the Straits of Hormuz or Malacca (Cooperative Association for Internet Data Analysis, 2009). The security of these critical nodes—some of which may be physical, others informational—

³ Dodge and Kitchin (2001) conducted a 5-year study of cyberspace maps and spatializations created by academic and commercial organizations and compiled their results in *Atlas of Cyberspace*.

should be of great interest to anyone attempting to protect or exploit cyberspace.

Given such similarities among the two strategic commons, cyberspace has at least five unique characteristics of concern to senior security leaders. First, the cost of entry and routine access to cyberspace is extremely low—basically the cost of a laptop and Internet café fee. Second, cyberspace offers a degree of anonymity that greatly challenges efforts to detect, track, and target a user who desires to hide in the common.⁴ Third, cyberspace provides the ability to initiate a wide variety of physical effects across vast distances at almost instantaneous speeds. Fourth, cyberspace is an ever-growing common—every new computer server or Internet-capable cell phone expands its boundaries. Finally, cyberspace does not have traditional dimensions of height, depth, and length, but it does have unique metrics that can be used to map its boundaries and operations.⁵

What types of threats exist in this new common? In general, attacks in cyberspace fall into one of three categories—the interception, modification, or denial of information (Woolley, 2006). Attacks may be overt or covert, with kinetic or nonkinetic effects. The damage inflicted varies greatly, from defaced Web sites to multi-million-dollar financial losses, and even to actual physical damage to equipment, the control of which is connected to cyberspace. How do leaders transform their organizations to address these challenges?

Organizations and the Cyberspace Process

The United States clearly recognizes that cyberspace security (also called cybersecurity) is essential to its overall national security and that it has implications across all instruments of national power—diplomatic, informational, military, and economic. The U.S. strategic

⁴ Some may argue that individuals may hide in physical space among a population of billions with equal anonymity, such as that offered by cyberspace. Although a full debate exceeds this chapter's scope, some of the unique features facilitating anonymity in cyberspace include the ability to enter and exit the common, the ability to create and control multiple versions of the user's presence, and the ability to take over another user's identity (usually without their consent or knowledge)—all accomplished with no change to the user's actual physical attributes.

⁵ Note that this is one area where the author disagrees with Cebrowski's view that the cyberspace common is dimensionless (Cebrowski 2004).

objectives for accomplishing this security are to prevent cyberattacks, reduce national vulnerability to cyberattacks, and minimize damage and recovery time, should attacks occur. Equally important, the need to have a secure cyberspace involves the international community. The United States explicitly states this in two of its five national priorities for its cyberspace strategy—securing governments' cyberspace and international cooperation (Bush, 2003).

This section addresses how organizations interact and innovate to transform their own structures to meet the security challenges of cyberspace. The discussion steps through each of the four major instruments of national power to assess their status and identify issues for senior security leaders to comprehend and work to resolve.

Diplomatic

How should countries interact in cyberspace? Does this new common require entirely new standards of conduct? As independent governments, they have an international obligation to act in good faith and settle disputes with other states by peaceful means. If conflict should occur, the right of using proportional force in self-defense is a cornerstone of international security. Sharp (1999) argues that “it now seems almost universally accepted that a considerable body of international law does indeed apply to the use of force by states in CyberSpace.”

However, the widely distributed nature of cyberspace does not necessarily recognize national boundaries, and new provisions to address this reality seem prudent. Arguably, the most significant event moving us toward defining acceptable cyberspace interactions is the Council of Europe Convention on Cybercrime, a formal agreement among 43 countries “to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation” (Archick, 2006, 1). The convention began in 1997, was opened for signature on November 23, 2001, and has been ratified by at least 16 countries. Its provisions include definition of criminal offenses in four categories (fraud and forgery, child pornography, copyright infringement, and security breaches), as well as methods to address these crimes, such as investigation and extradition procedures (Archick, 2006).

The U.S. Department of Justice has arrested and convicted domestic and international individuals and small groups committing cyberspace-

related crimes since 1998.⁶ The department determines whether the crime targeted a private individual or corporation or a government agency, as well as whether the crime posed a threat to public health or safety (e.g., power grids, air traffic control) (U.S. Department of Justice, 2009). The attackers included citizens from China, Russia, Kazakhstan, Israel, and the United Kingdom. In some cases, extradition requests were pursued per the Convention on Cybercrime (Anonymous, 2009).

Informational

How can information be stored safely in cyberspace? The U.S. Government views information technology as one sector of the nation's critical infrastructure and has tasked the Department of Homeland Security with its protection. In turn, the Department of Homeland Security created a National Cyber Security Division in June 2003 to serve as a focal point for cybersecurity issues. Working to avoid information-sharing failures such as those that contributed to the September 2001 terrorist attacks, the Department of Homeland Security conducted 16 major cyber exercises between 2004 and 2008. To practice and enhance collective responses to cybersecurity scenarios, the exercises included participants from federal, state, and local governments, as well as participants from private industry, academic institutions, and foreign governments (U.S. Government Accountability Office, 2008).⁷

In January 2008, President Bush signed Homeland Security Presidential Directive 23, better known as the Comprehensive National Cybersecurity Initiative. The initiative is a classified document, but three of its major "public" priorities directly support the access points, data traffic, and security protocol for information traversing U.S.

⁶ The fact that the U.S. Department of Justice claims jurisdiction for cyberspace crimes having physical effects on U.S. individuals and organizations is not the same as suggesting there is a "U.S. cyberspace boundary." The details of physical and virtual national sovereignty deserve further debate.

⁷ Cyber Storm II description: Sponsored by the Department of Homeland Security, this exercise was to improve national incident response and coordination capabilities by simulating physical and cyber attacks against the transportation, information technology, and chemical critical infrastructure sectors. Participants included federal, state, and foreign governments and private industry (General Accounting Office, 2008).

Government agencies' computer networks. First, the Trusted Internet Connection effort is simply a way to prevent cyberattacks by reducing the number of access points. Next, the Einstein II program automatically monitors the data traffic within the networks and Internet access points. Third, the Federal Desktop Core Configuration program mandates a common security protocol for government desktop computer systems (Lake, 2009).

Military

How are traditional military organizations embracing operations within the cyberspace domain? In his recent testimony before the U.S. Congress, Secretary of Defense Robert Gates (2009a, 8) acknowledged the extent of the threat:

With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid—a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million [information technology] devices.

To address this issue, Secretary Gates designated cyberspace as one of the four focus areas in the recent Quadrennial Roles and Missions Review (Gates, 2009b), a reinforcement of tenets in his 2008 National Defense Strategy (Gates, 2008). The goal is to establish the foundation for developing capable cyberspace forces; structure the forces, as well as their processes and procedures; and then employ these forces to achieve desired effects across the full range of military operations. The study's Cyber Issue Team emphasized the need "to learn from new, innovation capabilities and experiences of our counterparts across the U.S. Government, in the private sector, and internationally" (Gates 2009b, 16).⁸

In April 2007, the Estonian government, commercial, and private organizations endured 3 weeks of cyberattacks. Responding to a historic request by a member state of the North Atlantic Treaty Organization (NATO) in defense of its digital assets, the United States sent computer security experts to Estonia to help with recovery efforts

⁸ The stated Department of Defense vision is to develop cyberspace capability that provides global situational awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and when called on, provide cyberspace support to civil authorities (Gates 2009b, 14).

(Geers, 2008). The aftermath of this attack included the creation of two new cybersecurity organizations. First, at the operational level, the Cyber Defence Management Authority was established in Brussels, Belgium, to provide a centralized bureau for coordinating Alliance response to any further cyber attacks (Hughes, 2009). Second, at the strategic level, the Cooperative Cyber Defence Centre of Excellence was established at Tallinn, Estonia, with a mission “to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance’s interoperability in the field of cooperative cyber defence” (Cooperative Cyber Defence Centre of Excellence, 2009).

Economic

What are the costs to industry of cybersecurity breaches? How can these costs be quantified and evaluated so business firms can adopt the measures that provide the most cost-effective solution? The stakes are high—a recent report surveying senior information technology decision-makers from over 1,000 large businesses and security firms estimated that companies lost an average of US\$4.6 million worth of intellectual property in 2008 (McAfee, 2009). The latest Annual Threat Assessment of the Intelligence Community estimates total cyber-related business losses in 2008 to be US\$42 billion for the United States and US\$140 billion globally, as well as possibly US\$1 trillion worth of intellectual property lost globally (Blair, 2009). Even determining when an attack occurs in business is difficult, and it is even more challenging to measure the cost of attacks. However, investigations into effects on stock price following cyberattacks indicate that targeted firms suffer short-term losses of 1% to 5%, which could translate into shareholder losses of as much as US\$200 million (Cashell et al., 2004).

Three major market forces compel businesses to manage their cybersecurity—competition, liability, and insurance. Firms that establish best practices for cybersecurity will be rewarded in a competitive market. Reduced cyberattacks lead to increased consumer confidence, as well as a healthy net profit. If these benefits are not sufficient, then liability, specifically the prospect of potential legal actions for compromised confidential consumer information, is a strong motivation. Finally, profit opportunities are emerging for cyber-risk insurance. Both the company buying such insurance and those supplying the service stand to profit, as they have in similar economic ventures (Cashell et al., 2004).

Cyberspace Issues for Organizational Transformation

How should senior security leaders address the challenges posed to current organizations by the dynamic activities in cyberspace? Will traditional approaches and structures suffice, or are new organizations required? Rather than delve down to the tactical level, let us address these questions at the strategic level, focusing on three tenets—credibility, balance, and hierarchy of organizational transformation to incorporate cyberspace.

From the preceding discussion, it is clear that security in cyberspace is an issue affecting all instruments of national power. The recent report, *Securing Cyberspace for the 44th Presidency* (Langevin et al., 2008, 15), lists as one of its three major findings that, “The United States must treat cybersecurity as one of the most important national security challenges it faces. ... This is a strategic issue on par with weapons of mass destruction and global jihad.”

If organizations are to achieve credibility in such security efforts, then they need to articulate the expressed risks in consistent and objective terms. For example, when cyberspace is viewed as the new strategic common, comparing security in cyberspace to issues like weapons of mass destruction is no more applicable than a comparison with security of the sea. Perhaps a way to articulate security issues for cyberspace more effectively is to couple the strategic common construct with the current U.S. model of challenges—traditional, irregular, disruptive, and catastrophic (Rumsfeld, 2006). Although there are, no doubt, potential “nightmare scenarios” that can be constructed within cyberspace, their roles need to be assessed objectively by considering the possible outcome in concert with its feasibility and probability of occurrence. Then the concern expressed in the previous quotation can be reworded to achieve credibility of purpose; “Although unlikely, the catastrophic cyber attack on our military networks is a strategic issue on par with weapons of mass destruction.”

Unlike the other strategic commons, cyberspace has direct and regular interface with a vast numbers of people in over two hundred countries (Central Intelligence Agency, 2008). At a United Nations Internet Governance Forum in November 2007, a key participant noted, “the dilemma between Internet freedom and Internet regulation could be resolved by striking a balance among the various competing interests” (U.N. News 14 November 2007). In this context, the opposing sides of the scale are security versus personal privacy.

Despite the international security benefits achieved by the Cybercrime Convention, some organizations petitioned U.S. senators to oppose its ratification, asserting it “lacks adequate safeguards for privacy” and has “insufficient recognition of international human rights obligations” (Rotenberg & Laurant, 2005). Although this opposition did not prevent ratification, its espoused principles deserve continued attention by strategic leaders as they transform organizations. Consistent with this, the October 2007 U.S. National Strategy on Information Sharing specifically establishes “Protecting Privacy and other Legal Rights” as its foundation, which includes foreign partners in this tenet. In addition, it explicitly links these principles to the pursuit of other national strategies, including homeland security and combating terrorists (Bush, 2007).

How should senior security leaders organize their resources to address the full spectrum of cybersecurity challenges? In an ironic twist, a recent report (Langevin et al., 2008) recommended in general terms that the U.S. Government move toward an information-age government that uses cyberspace and social networking, yet the report also recommended at least five new industrial-age organizations in the short term. Conti and Surdu (2009) argue for a new cyberwarfare branch of the U.S. military but fail to articulate what mission it would fulfill. It is doubtful that such traditional bureaucratic structures can keep pace with the rapidly evolving nature of cyberspace. Arquilla and Ronfeldt (2001, 15) are direct in their assessment: “hierarchies have a difficult time fighting networks,” and groups organized in networks pose many of the challenges in cyberspace. Although more responsive and better suited for countering dynamic threats, transforming current security organization into network-based structures requires leaders who are comfortable with flexibility and dispersed authority.

People and the Cyberspace Process

Having looked at the various organizations and instruments of power at work within cyberspace, let us consider the individuals who operate there. This section first focuses on people who choose to conduct illegal activity in cyberspace. Next, it examines the connectivity and attitudes of people using cyberspace and concludes with a look at various factors affecting the mutual transformation of people and the cyberspace strategic common.

Wrongdoers in Cyberspace

Who are the perpetrators of illegal activity in cyberspace? To analyze the diversity of cyberspace lawbreakers, let us consider four categories of these individuals (who may also work in groups)—cyber-delinquents, cybercriminals, cyberspies, and cyberterrorists. Each set of perpetrators differs in attitudes and actions regarding ideology (e.g., political or religious), monetary gain, attribution, knowledge-sharing, and destruction of societal structures. One common interest among all but the most extreme individuals (e.g., anarchists) is the preservation of cyberspace infrastructure—they all have a vested interest in maintaining the domain from which they derive power.

Think of cyber-delinquents as the thrill seekers of cyberspace. Their primary motivation is to cause trouble that is highly visible in cyberspace, and perhaps in the world in general as well. To demonstrate their brilliance and “share the fun,” they are more likely to provide their trade secrets for beating cyberspace security. Ideology and monetary gain may play a role in their psyche, but they do not dominate. Although not their intent, some of their pranks may inadvertently endanger public safety (e.g., changing traffic signals) or violate very severe laws, such as possible child pornography in the recent cases of “sexting” among teens (Hamill, 2009). In the grand scheme of cyberspace security, cyber-delinquents are regrettable nuisances.

In contrast, consider cyber-criminals, operators focused primarily on monetary gain. They have little regard for ideology and destruction of societal infrastructure unless they are acting in a mercenary role. Obviously, they do not want to be known, as that increases their probability of arrest, and they are not apt to share the techniques they use to turn a profit. In strategic terms, they are a growing threat to economic power. The 2008 CSI Computer Crime and Security Survey noted the disturbing trends of cybercriminals becoming more professional in their crimes, clearly separating themselves from cyber-delinquents’ pursuit of “bragging rights.” Cybercriminals have become stealthier by exploiting the inherently reactive nature of defensive security measures, as well as more sophisticated in the targeting of their attacks. The most expensive attacks were those of financial fraud, with an average reported cost of over US\$463,000 per incident (Richardson, 2008). In broader terms, criminals stole data from over 47 million credit and debit cardholders by hacking retail marketers (Housman, 2009).

Next are the cyberspies—operators driven by ideology, usually of a specific government. Similar to the cybercriminals, they seek to remain anonymous in their deeds and capabilities, but they may share information with other cyberspies for mutual benefit. They may cause no overt damage in their activities, opting to monitor information rather than intercept it. By constantly probing and scanning critical nodes of other countries' cyberspace infrastructure, they can identify vulnerabilities to be extorted or exploited during a time of crisis or conflict. The scope of such activity is staggering. Wilson (2008) cites U.S. Department of Defense officials' estimates of the military global information grid experiencing more than three million daily scans, as well as counterintelligence officials' estimate that 140 different foreign intelligence agencies regularly attempt to hack into U.S. commercial and government computers.⁹

Finally, there are the cyberterrorists, who are motivated by political or social ideology but also by the desire to be recognized for their deeds to aid in recruiting followers or gaining perceived legitimacy (including possible state sponsorship). They work effectively in a network structure and are likely to share much of their knowledge regarding how to conduct terrorist operations in the hope of spreading their influence. Monetary gain through cyberspace crimes may not be a direct motivation for cyberterrorists, but it may help fund their activist agendas. Because they can exercise significant power and influence through cyberspace, one could argue that it is unlikely that they will cause widespread damage to its supporting infrastructure.

Connectivity

Innovations in computer technology have greatly enhanced the ability of the average citizen to operate freely in cyberspace. Data processing speeds and digital storage media continue to grow exponentially (Ekman et al., 2004), with competitive markets that drive sales prices down. The United States accounts for over 22% (over 264 million) of all personal computers in the world (over 1.19 billion; Computer Industry Almanac, 2009), but China recently surpassed the United States in the number of Internet users (253 million versus 220

⁹ In April 2009, the *Wall Street Journal* reported alleged activities in which cyberspies from China, Russia, and other countries “were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war” (Gorman 2009).

million; Anonymous, 2009). With 222 countries having Internet access, 86 of which have at least one million users (Central Intelligence Agency, 2008), it is becoming difficult to find any place in the world not affected by cyberspace. In fact, the United Nations recently sponsored an Internet governance conference with attendees from over 100 governments, with two of the five main topics focused on “reaching the next billion with Internet access” and “the Internet of tomorrow” (U.N. News, 2008b)

Because the cyberspace process includes physical elements, it is not surprising that industry and government leverage the ability of cyberspace-based remote access to control infrastructure. Usually called Supervisory Control and Data Acquisition (SCADA) systems, these control processes increase operational effectiveness and efficiency for many applications to include such systems as electric power, oil, gas, transportation, and telecommunications (Varnado, 2005). Often, older SCADA devices were designed and installed without regard for security, and most new SCADA systems use the Internet to pass control information. As the worldwide population of Internet users pushes toward two billion, it is wise to pursue better security promptly for any physical systems accessible via that portion of cyberspace.¹⁰

Attitudes

Is the increasing individual and collective access to cyberspace creating its own unique cyber-ethos? How is this transforming the interactions among people and groups? Certainly, the current generation of Internet users is diverse, but many are using cyberspace to bridge gaps in language and culture. Social networking Web sites, such as Facebook and MySpace, attract around 115 million unique visitors each month, demonstrating a willingness to place personal information online (Arrington, 2008). There are also many new avenues of immediate communication available to users—such as instant messaging, blogs, and Twitter—that are accessible through a myriad of hard-wired as well as wireless devices (e.g., cell phones, personal digital assistants, laptops, etc.).

¹⁰ The U.S. Department of Energy reported on recommended changes to power-generation facilities resulting from a U.S. Department of Homeland Security experiment in March 2007. The test demonstrated the ability to cause catastrophic physical damage to an industrial turbine via commands sent through its SCADA system (DOE 2007).

The ubiquitous nature of the virtual social world facilitated by these devices often causes problems in “real” society. In the interest of public safety, many U.S. states outlawed the use of cell phones for motor vehicle drivers, and sometimes the law specifically restricts text messaging (Governors Highway Safety Association, 2008). The potentially devastating effects of “cyber bullies” are also being scrutinized, especially in light of tragic events where it may have contributed to an individual’s death, such as a recent teenage suicide in Missouri (CBS News, 2008). It is reasonable to expect new social and ethical issues for the cyberspace common as it continues to expand into global society.

Cyberspace Issues for Transforming People

Does the transforming nature of cyberspace present new challenges for senior security leaders in their interactions with people, or will status quo interpersonal dynamics suffice? To evaluate this, let us focus on three strategic topics—trends, leverage, and synthesis of technologies and individuals—and the implications of transforming their interactions in cyberspace.

At risk of stating the obvious, it is important for senior security leaders to realize and embrace the future trends of cyberspace. With regard to people, they must fully understand the ramifications of the current generation of students entering university. Given the start of modern cyberspace posited in this essay, these students know no other world than that of billions of computers and Internet users. What is a revolution for senior leaders is status quo to them.

Consider the recent U.S. presidential election. BBC News (Schiffers, 2008) reported on Barack Obama’s campaign success in using the Internet for fundraising and communication as representing a sharp departure from traditional phone call tactics. Although viewed as innovative among older voters, newly registered voters may respond simply, “Of course these techniques were used—how else do you communicate?” This example illustrates how different generations view and apply readily available cyberspace tools. As senior leaders seek to recruit and develop people in their organizations, they should not limit their focus to fulfilling the needs of today’s cyberspace activities but, rather, should look at least several decades into the future to envision and pursue the talents and skills required for a transformed cyberspace common. However, they need to remember that not everyone operating in cyberspace has lawful motives.

What types of skills and technology can people leverage to their advantage within cyberspace? Individuals in the four broad categories of cyberspace wrongdoers may interact for mutual benefit, or they may exploit law-abiding operators. Wilson (2008) identifies cases in which cyberterrorists employed cybercriminals to steal credit card information and support drug traffickers, all toward the goal of funding traditional terrorist operations. Another lucrative business is the marketing of “botnets”—virtual armies of compromised computers that can be controlled remotely over the Internet by a “botmaster.” Botnets may exploit hundreds of thousands of computers, usually without the owners’ knowledge (Wilson, 2008). An adversary with such capability, if coupled with a network structure, could achieve swarming attacks and defenses—in cyberspace as well as other strategic commons—that challenge the “traditional mass- and maneuver-oriented approaches to conflict” (Arquilla & Ronfeldt, 2001, 12).

As the cyberspace capabilities increase, the methods used to develop individual skills to leverage these capabilities transform. User interfaces have progressed significantly over the past two decades, incorporating visual icons and common menu structures that allow even novice users the ability to master new applications in hours, if not minutes, without any formal training. If problems occur, the “help” menus offer advice and tutorials, often supported by extensive online databases. Unfortunately, not all “self-help” is benevolent. Cyber wrongdoers can develop and enhance their illegal skills using online “how to” information that may be updated rapidly to counter new security measures. To meet this challenge, senior leaders may need to transform traditional education, training, and certification programs for their cybersecurity workforce and emphasize continuous training using decentralized network techniques. As Arquilla and Ronfeldt (2001, 15) concluded, “whoever masters the network form first and best will gain major advantages.”

How will people and their leaders cope with the cyberspace common’s expansion, as well as its supporting technologies that grow at geometric rates? Although existing WiFi and Bluetooth technologies have removed the bonds of cables and lines for many users, ongoing research and development offers further possibilities for removing cumbersome computer display and input devices. This ultimate degree of connectivity with almost no personal physical infrastructure is still ahead, perhaps in the near future.

Consider the synthesis of combining proven and feasible technologies to enhance the human–machine interface. Over 112,000 people worldwide have cochlear implants—a transmitter and receiver device that stimulates the auditory nerve in deaf patients to simulate nature hearing processes (National Institute on Deafness and Other Communication Disorders, 2007). Similar principles were used to develop a self-contained artificial silicon retina microchip, which is implanted in the human eye to help mitigate retinal degeneration (Optobionics, 2008). Starner and Paradiso (2004) present several viable options for human-generated power for operating mobile electronics, most based on normal body motion (e.g., walking, breathing, body heat, etc.). By combining these technologies and adding fingertip sensors for data entry purposes, it is conceivable that their synthesis could result in people who have a fully self-contained direct interface to cyberspace. Certainly, this could raise even more challenging issues of security and privacy, given the potential for every individual with optical implants to become a walking Web camera.¹¹

If this ultimate connectivity comes to fruition, it may have pronounced effects on many individuals. A survey by Anderson and Rainie (2006) postulates it may exacerbate two extreme attitudes within the population—addicts and luddites. The addicts are those individuals who devote most of their time to living in synthetic worlds. Often disguising their true nature and characteristics by appearing as self-designed “avatars,” the prospect of almost complete sensory immersion into cyberspace may cause them to retract further from real-world society. In contrast, luddites are individuals who oppose technological change. The radical measures of achieving ultimate connectivity may create such a change in society as to compel violence from such individuals who refuse to participate. Some in the survey also worried that technology may eventually create machines and processes that move beyond human control. Although this notion has been the theme of many works of fiction over more than a century, the continued rapid growth of cyberspace systems’ capability and complexity now makes it a legitimate concern for organizational leaders.

¹¹ Perhaps the most radical approach in such an environment would be to adopt a doctrine of total transparency—basing plans and operations on a central assumption that all users can see all information at any time. Although thought provoking, the implications of this concept are beyond this chapter’s scope.

Conclusion

Clearly, the dawn of modern cyberspace introduced a myriad of challenges, only a small sample of which were discussed in this essay. I offer five closing thoughts on the central theme of what senior security leaders must know about cyberspace to transform their organizations and make wise decisions. First, they should avoid the mystery surrounding cyberspace and embrace it as a new strategic common of communication and commerce akin to the sea. They should recognize and plan for its security across all instruments of national power—diplomatic, informational, military, and economic. Next, it is doubtful that existing hierarchies will be effective in achieving cybersecurity against networked adversaries. Leaders need to consider adopting similar dispersed network principles to transform their organizations to be more agile and less vulnerable. Third, leaders should not lump all adversaries together but, rather, recognize that they may have common motivations and self-imposed restrictions regarding how they operate in cyberspace. These groups have the capability to interact over vast distances with each other as well as to exploit unwilling users in ways that increase their collective ability to affect cyberspace operations. Next, although there is a trend toward greater sharing of personal information via social networking, the measures that leaders direct to meet cyberspace challenges need to balance the efficiency and effectiveness of security against the universal laws of privacy and human rights. Finally, leaders need to scan the strategic horizon for potential cyberspace-related technological and societal trends and shocks and provide clear visions for success to their organizations.¹²

¹² Since the original presentation of this essay, three significant events have occurred in the United States. First, on May 29, 2009, President Obama announced the creation of a new White House office led by a Cybersecurity Coordinator as well as five key areas for action. The coordinator will be a member of both the National Security Staff and the National Economic Council. It is interesting to note that President Obama mentioned that his staff's computers were hacked during the general election campaign (Obama 2009). Second, on June 23, 2009, Secretary of Defense Gates directed the development of a new national strategy for cybersecurity as well as the establishment of U.S. Cyber Command as a subordinated unified command under U.S. Strategic Command. He specified an initial operating capability not later than October 2009 and full operating capability by October 2010 (Gates 2009c). Third, on July 4, 2009, there was a wave of cyberattacks aimed at American and South Korean government and commercial Internet sites.

References

- Anderson, J.Q. & Rainie, L. (2006). *The Future of the Internet II*. Washington, DC: Pew Internet and American Life Project. Available from <http://www.pewinternet.org> [Accessed March 31, 2009].
- Archick, K.. (2006). *Cybercrime: The Council of Europe Convention*. CRS Report for Congress RS21208. Washington, DC: Congressional Research Service.
- Arquilla, J. & Ronfeldt, D. (2001). "The Advent of Netwar (Revisited)," in Arquilla and Ronfeldt, eds. *Networks and Netwars*. Santa Monica, CA: RAND, 1–25.
- Arrington, M. (2008). "Facebook No Longer The Second Largest Social Network." *Tech Crunch* June 12. Available from <http://www.techcrunch.com> [Accessed April 1, 2009].
- Blair, D.C. (2009). *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*. Washington, DC: Director of National Intelligence.
- Bush, G.W. (2003). *The National Strategy to Secure Cyberspace*. Washington, DC: White House.
- Bush, G.W. (2007). *National Strategy for Information Sharing; Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: White House.
- Cashell, B. et al. (2004). *The Economic Impact of Cyber-Attacks (CRS Report for Congress RL-32331)*. Washington, DC: Congressional Research Service.
- CBS News. (2008). "Woman Indicted in Cyber-Bully Suicide." May 15. Available from <http://cbsnews.com> [Accessed April 1, 2009].
- Cebrowski, A.K. (2004). "Transformation and the Changing Character of War? Transformation Trends." Available from <http://www.afei.org/transformation> [Accessed March 27, 2009].
- Central Intelligence Agency. (2008). "Country Comparisons—Internet Users," in *The World Factbook*. Available from <https://www.cia.gov/library/publications> [Accessed March 31, 2009].

Officials and experts stated that at least 27 sites were targeted by botnets of 50,000 to 65,000 computers. Assessments of the attack ranged from "unusually resilient" to "garden-variety" (Sang-Hun & Markoff 2009).

- Computer Industry Almanac. (2009). "PCs In-Use Reached nearly 1.2B in 2008; USA Accounts for Over 22% of PCs In-Use." News Release January 14. Available from <http://www.c-i-a.com> [Accessed March 31, 2009].
- Cooperative Association for Internet Data Analysis. (2009). *Data Collection at CAIDA—Research Topics*. San Diego, CA: Cooperative Association for Internet Data Analysis. Available from <http://www.caida.org/data/> [Accessed March 31, 2009].
- Cooperative Cyber Defence Centre of Excellence. (2009). *Mission and Vision*. Tallinn: Cooperative Cyber Defence Centre of Excellence. Available from <http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD> [Accessed March 30, 2009].
- Claffy, K. et al. 2008. *Internet Mapping: From Art to Science*. San Diego, CA: Cooperative Association for Internet Data Analysis.
- Conti, G. & Surdu, J. (2009). "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" *IAnewsletter*, 12(1), 14–17.
- Dodge, M. & Kitchin, R. (2001). *Atlas of Cyberspace*. Harlow: Pearson Education.
- Ekman M. et al. (2004). *An In-Depth Look at Computer Performance Growth (Technical Report 2004-9)*. Goteborg: Chalmers University of Technology.
- England, G. (2008). "Memorandum: The Definition of 'Cyberspace.'" Washington, DC: Department of Defense.
- Gates, R.M. (2008). *National Defense Strategy*. Washington, DC: Department of Defense.
- Gates, R.M. (2009a). "Submitted Statement to Senate Armed Services Committee (January 27, 2009)." Washington, DC: U.S. Senate.
- Gates, R.M. (2009b). *Quadrennial Roles and Missions Review Report*. Washington, DC: Department of Defense.
- Gates, R.M. (2009c). Memorandum, June 23, 2009. "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Washington, DC: Department of Defense.
- Geers, K. (2008). *Cyberspace and the Changing Nature of Warfare (IST-076/RSY-017)*. Tallinn: Cooperative Cyber Defence Centre of Excellence.
- Gibson, W. (1984). *Neuromancer*. New York: Ace Books.
- Gorman, S. (2009). "Electricity Grid in U.S. Penetrated By Spies." *The Wall Street Journal*, April 8. Available from <http://online.wsj.com> [Accessed May 3, 2009].

- Governors Highway Safety Association. (2009). "Cell Phone Driving Laws." Available from <http://www.ghsa.org> [Accessed April 1, 2009].
- Hamill, S.D. (2009). "Students Sue Prosecutor in Cellphone Photos Case." *New York Times*, March 26. Available from <http://www.nytimes.com> [Accessed March 30, 2009].
- Housman, R. (2009). "The Cyber Secure Institute." *Homeland Defense Journal*, 6(7), 17.
- Hughes, R.B. (2009). "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief*, 1, 4–8.
- Internet World Stats. *Top 20 Countries with the Highest Number of Internet Users*. Available from <http://www.internetworldstats.com> [Accessed March 31, 2009].
- Lake, B. (2009). CyberThreats: A Cultural Change of Combating Threats. *Homeland Defense Journal*, 6(7), 14–16.
- Langevin, J.R. et al. (2008). *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies.
- London, England Hacker Indicted Under Computer Fraud and Abuse Act for Accessing Military Computers*, 2009. Washington: Department of Justice. Available from <http://cybercrime.gov/mckinnonIndict.htm> [Accessed March 24, 2009].
- McAfee. (2009). *Unsecured Economies: Protecting Vital Information*. Santa Clara, CA: McAfee
- National Institute on Deafness and Other Communication Disorders. (2007). *Cochlear Implants*. Available from: <http://www.nidcd.nih.gov/health/hearing> [Accessed April 1, 2009].
- Obama, B.H. (2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Washington, DC: White House.
- Optobionics. (2008). *ASR Device*. Available from <http://www.optobionics.com> [Accessed April 1, 2009].
- Richardson, R. (2008). *CSI Computer Crime & Security Survey*. Computer Security Institute.
- Rotenberg, M. & Laurant, C. (2005). "EPIC Statement on COE Cybercrime Convention, Treaty 108-11." Letter to Senators Lugar and Bidden, July 26, 2005.
- Rumsfeld, D.H. (2003). *Transformation Planning Guidance*. Washington, DC: Department of Defense.

- Rumsfeld, D.H. (2006). *Quadrennial Defense Review Report*. Washington, DC: Department of Defense.
- Sang-Hun, C. & Markoff, J. (2009). "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *The New York Times*, July 10. Available from <http://www.nytimes.com> [Accessed July 14, 2009].
- Schifferes, S. (2008). "Internet Key to Obama Victories." BBC News. Available from <http://newsvote.bbc.co.uk/> [Accessed April 1, 2009].
- Sharp, W.G. Sr. (1999). *CyberSpace and the Use of Force*. Falls Church, VA: Aegis Research.
- Starner, T. & Paradiso, J.A. (2004). Human Generated Power for Mobile Electronics.
- U.N. News. (2008a). "UN Forum Tackles Balance Between Property Rights and Internet Freedom." Available from <http://www.un.org/news/> [Accessed March 30, 2009].
- U.N. News. (2008b). "UN Forum Wraps Up With Call for Collaboration to Achieve 'Internet for All.'" Available from <http://www.un.org/news/> [Accessed March 30, 2009].
- U.S. Department of Energy. (2007). "Experiment Showed Grid Vulnerability to Cyber Attack—Flaws Fixed." *Energy Assurance Daily*, September 27. Available from <http://www.oe.netl.doe.gov/> [Accessed May 7, 2009].
- U.S. Department of Justice. (2009). *Computer Crime Cases*. Washington, DC: Department of Justice. Available from <http://www.cybercrime.gov/cccases.html> [Accessed March 24, 2009]
- U.S. Government Accountability Office. (2008). *Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise (GAO-08-825)*. Washington, DC: Government Accountability Office.
- Varnado, S.G. (2005). *SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems*. Washington, DC: U.S. House of Representatives.
- Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (CRS Report for Congress RL-32114)*. Washington, DC: Congressional Research Service.
- Woolley, P.L. (2006). *Defining Cyberspace as a United States Air Force Mission*. Master's Thesis, Air Force Institute of Technology.