CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 31 / CCEM 31

UNTANGLING THE WEB: BALANCING SECURITY, PROSPERITY, AND FREEDOM IN THE INFORMATION AGE.

By /par Maj J. Reitz, U.S. Army
Syndicate 9
May 2005

TABLE OF CONTENTS

DEDICATION

I would like to dedicate this paper to the men and women who serve daily to protect our nation and our freedoms, especially for those who have paid the ultimate price. I pray that this paper would honor their sacrifice to maintain the precious equilibrium between freedom and security. For their sake and for that of our children, we must get it right. It is my sincere hope that this paper adds clarity to the discussion of the delicate balance between security and privacy in the Information Age.

ABSTRACT

In less than three decades the Internet has grown from a small network of university and government computers to a global, interconnected web of computers of mind-boggling proportion. In the interceding years, the United States has grown increasingly dependent on the ability of computers to process and share information over the Internet. Enabled by tremendous gains in computing power and a growing number of interconnected databases that house information, individual privacy as well as national security are being threatened in ways that were unimaginable fifty years ago. Furthermore, the growing compartmentalization of *sensitive but unclassified* data is limiting state and local first responders from access to important information and is diminishing citizen awareness of government action.

In order to mitigate the risks posed to society by threats to information security the U.S. government should establish standards for a national Internet identity card. While the proposal of any sort of "national identity card" raises significant privacy concerns, this paper argues that, if applied properly, a national standard would actually enhance Americans' privacy and security in the information age.

INTRODUCTION

In less than three decades the Internet has grown from a small network of university and government computers to a global, interconnected web of computers of mind-boggling proportion. In the interceding years, the United States has grown increasingly dependent on the ability of computers to process and share information over the Internet. Enabled by tremendous gains in computing power and a growing number of interconnected databases that house information, individual privacy as well as national security are being threatened in ways that were unimaginable fifty years ago. Furthermore, the growing compartmentalization of *sensitive but unclassified* data is limiting state and local first responders from access to important information and is diminishing citizen awareness of government action.

If left unchecked, these two factors could erode the very purpose of the nation, "to establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty".[1] Conversely, these dynamics, if harnessed imaginatively can serve to enhance our nation's physical security, economic well-being, and individual privacy.

In order to mitigate the risks posed to society by threats to information security the U.S. government should establish standards for a national Internet identity card. While the proposal of any sort of "national identity card" raises significant privacy concerns, this paper argues that, if applied properly, a national standard would actually enhance Americans' privacy and security in the information age.

---

[1] *The Constitution of the United States* [Internet] (Heritage.org, 1789 [cited 14 Feb 2004]); available from http://www.heritage.org/.

The first chapter provides a short history of computing and how it has changed our world. Chapter two describes the various threats to those who depend upon computers and the Internet to process, store, and transmit data. Chapter 3 explores the U.S. Government's approach to securing the nation's information infrastructure, and the last chapter offers a solution that strikes a balance between individual liberty and national security.

1 – INFORMATION & POWER

Enigma, the IBM PC, & HTML

Early in World War II the Allies captured a German "Enigma" encryption device but did not know the daily settings which allowed the device to decrypt the messages sent by the German high command to its subordinates. In order to solve this problem, British scientists developed the precursor to the modern computer. The machine enabled the Allies to decrypt Enigma's daily code in as little as 15 hours. Today, the machine on which this paper is being written can do the same task in a matter of minutes.[2]

It was the advent of mainframe computer in the late 1960s that brought the information age to the forefront, however. These machines allowed both government and industry to process and store large amounts of data automatically. By the mid-1970s computers were commonplace in large corporations and government agencies. Scientists and programmers busied themselves to connect the hulking machines in order to facilitate the sharing of data to make information flow more efficient.

While corporations were content to connect their computers using dedicated phone lines, the Department of Defense had a peculiar need: redundancy in the event of a Soviet-launched nuclear strike. In 1968 the Defense Advanced Research Projects Agency (DARPA) contracted with two corporations to create a network that would enable high speed communications between military and university computers which

---

[2]*Cracking Enigma* [Internet] (ThinkQuest, n.d. [cited 19 April 2005]); available from http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/bombe.shtml, *Frequently Asked Questions About the Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors* [Internet] (National Institute of Standards and Technology, 2005 [cited 27 March 2005]); available from http://www.nist.gov/public_affairs/releases/piv_faqs.htm.

would not be easily disrupted by enemy saboteurs or nuclear weapons.[3] Initially known as the ARAPAnet, it would later become known just as, “The Internet”.

In order to do its job, the Internet was predicated on an entirely different protocol than that of the telephone network. While telephone networks allow two-way communications at the same time using “circuit switching”, each line is limited in use to

73 0 Tw 12 0 0 12 62688 598.55 5

limit the federal government's power to collect and store personally identifying data.[7] This legislation did nothing to prevent private corporations or even state and local governments from collecting and storing personally identifying data, however.

As the years passed, other sources, most of which were supported by the U.S. government came forward to add to the Internet infrastructure.[8] One crucial element to the later successes—and current challenges—of the Internet was to be the construct that defined the details of the communications protocol. Instead of the hierarchical circuit-based switching model found in the telephone network, the designers settled on creating an "open architecture". Under this construct, each sub-network could operate on its own, with a "gateway" which would allow entry onto the larger network. This would be the Internet. The various "gateways" of the Internet would work together to pass data along the most efficient route possible. This construct also had the effect of preventing censorship or control over data transmission. The design was open for all to use and anyone could offer their suggestions for improvement.

In 1981 the advent of the affordable home computer with its own microprocessor indelibly changed the face of computing and the Internet. Dubbed, "the PC" (Personal Computer), the International Business Machines Corporation (IBM) sold its first machine for $4500.[9] Computing was no longer limited to large corporations, government, or well-funded educational institutions. These first PCs, like their mainframe counterparts were connected to other computers through the Internet using cumbersome command-line

---

[7]*FOIA Reference Guide* [Internet] (Department of Justice, revised April 2005 [cited 27 April 2005]); available from http://www.usdoj.gov/04foia/04_3.html, *The Privacy Act of 1974: 5 U.S.C. § 552a* [Internet] (1974 [cited 27 April 2005]); available from http://www.usdoj.gov/04foia/privstat.htm.

[8]Opfer, *The History of the Internet According to Itself: A Synthesis of Online Internet Histories Available at the Turn of the Century*.

[9]Ibid.

prompts. The relative high cost of the PC and high learning curve effectively limited Internet use to those with a high degree of technical aptitude.

This all changed a decade later with the introduction of hypertext-transfer protocol (HTTP) and hypertext-markup language (HTML). HTTP and HTML allowed programmers to create hidden text and Graphical User Interfaces (GUI) through which even novice users could effortlessly "navigate". The advent of HTTP & HTML opened the doors of the Internet to the non-technically inclined through what was dubbed, by its founders, "the world-wide web (WWW)".[10] In addition to their PC and an Internet connection, users needed only a browser to view information over the web – which Netscape offered for free download in 1994.[11] Though the physical architecture of the Internet had not changed, the "web" lowered the barrier for entry onto the Internet to the education level of a kindergartner.

The end result has truly been revolutionary in the ways that organizations and governments communicate and conduct business. Anyone can publish anything, anytime, for a global audience. Business can be conducted automatically, 24 hours a day, every day of the year. Today, it is estimated that 63% of the American population (70 million) log on to the Internet daily to check email, get news, purchase goods, conduct research and engage in a myriad of other activities.[12] These figures make the United States the most connected nation on earth. Along with the newfound exchange of

---

[10]Ibid.

[11]Ibid.

[12]*A Decade of Adoption: How the Internet Has Woven Itself into American Life* [Internet] (www.pewinternet.org, 2005 [cited 20 April 2005]); available from http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf, 58.

knowledge inherent in the information age has also come a dynamic shift in the distribution of power.

Scientia potestas est

In the mid-15th century a wooden contraption with metal plates changed the Western world. The device was the Gutenberg moveable type printing press and is credited with sparking the Renaissance.[13] Though not the first work printed on the press, the now-famous Gutenberg Bible was instrumental in altering the power structure of medieval Europe. Prior to the Gutenberg press it took one monk 20 years to transcribe a copy of the Bible.[14] Furthermore, the only individuals able to read the Bible were the most learned within society.[15] As a result, an enormous amount of power rested with the Church hierarchy since it was the only intermediary to God. The moveable type press changed all the balance of power by pushing information to the common man. This early 'information revolution' fueled the protestant Reformation and ultimately reduced the power and influence of the Catholic Church.[16]

Several hundred years later the Industrial Revolution changed the demographics of society. People descended on cities in order to find work, and with the urbanization came increased opportunities for education. An educated populace demanded democracy, changing the balance of power once again.[17]

---

[13] *Wikipedia* [Internet] (Wikipedia, 2005 [cited 25 April 2005]); available from http://en.wikipedia.org/wiki/.

[14] Ibid.

[15] Alvin Toffler and Heidi Toffler, *Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century* (New York: Bantam Books, 1990), 84.

[16] Ibid., 413.

[17] Ibid., 11.

Within the span of 400 years, two information revolutions succeeded in radically altering the balance of power in the Western world. Today, only two centuries later, we have entered another information revolution. This time, however, the revolution is even more radical. In his influential book, *Powershift*, Alvin Toffler writes that there are five characteristics of this current information revolution which are unlike any change ever before in history: *interactivity*, *mobility*, *convertibility*, *connectivity*, *ubiquity*, and *globalization*.[18] Toffler predicts that these characteristics will result in a "…total transformation …in the way we think, how we see ourselves in the world, and therefore, where we stand in relationship; to our various governments." As a result, governments will lose their ability to "manage ideas, imagery, data, information, or knowledge as they once did."[19] While *brute force* and *wealth* are also components of *power*, the information age has changed the old dynamics. It is not that the other two components are no longer important, just that *information* has become preeminent.[20] As a result, "…the coming struggle for power will increasingly turn into a struggle over the distribution of and access to knowledge."[21] This is exactly the position in which we find ourselves today with private actors and governments straining for victory in an unending series of "information wars."[22]

---

[18]Interactivity refers to the way in which computers and humans now interrelate; Connectivity and Mobility are increasingly seen in modern wireless communications; Convertibility is similar to the definition offered earlier for *transportability*; and Ubiquity and Globalization refer to the coming of all-pervasive computing. Ibid., 359-60.

[19]Toffler argues that these factors played no small part in the late Soviet state losing control over its satellite states. Ibid., 413.

[20]Ibid., 20.

[21]Ibid.

[22] Ibid., 93-162.

These wars can have all sorts of casualties be they civilian, corporate, or governmental. Civilians lose privacy and sometimes their entire identity altogether; corporations and governments alike suffer from the results of information exploitation or all-out attacks by their adversaries.[23] As corporations and governments seek more and more information about people, corporations, and governments a resurgent need for secrecy arises.

This *powershift* has not been lost on the military which has branded operations in this realm, *Information Operations* (IO). IO has two components, Offensive IO and Defensive IO. While IO deals with information dominance as a whole, the subcomponent that deals with computers and networks is called Computer Network Operations (CNO). Offensive IO is the process of influencing the enemy's information systems. In the realm of computers and their associated networks this can take the form of Computer Network Attack (CNA) where the aim is to destroy or disrupt his systems, or Computer Network Exploitation (CNE) where the goal is to gather information from the adversary's computer systems in order to exploit the information. Finally, the process of defending one's own systems against CNA and CNE is called Computer Network Defense (CND).[24] One of the most fundamental means of defensive IO is the implementation of operational security (OPSEC).[25] The remainder of this paper is dedicated to the topic of CND in the Information age. In the following section we will examine some of the key characteristics of data in Internet-enabled era.

---

[23] Ibid.

[24] *DoD Directive 3600.1, Rev. 1: Information Operations (IO)* [Internet] (Department of Defense, 2001 [cited 28 April 2005]); available from http://www.iwar.org.uk/iwar/resources/doctrine/DOD36001.pdf.

[25] *FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures*, (Washington, D.C.: Headquarters, Department of the Army, 2003), v, 2-1.

Information: persistent, transportable, and universal

The Internet has transformed the way in which information is transmitted, processed, and stored. As a result, information has acquired some newfound attributes which deserve our attention. Unlike ever before, unless carefully guarded, information must be assumed to be *persistent, transportable,* and *universal.* No where is this better exemplified than in the World Wide Web (WWW). On the WWW 'web pages' are created on a *server* maintained by a *host*. Web pages are usually hosted by businesses whose job it is to keep its *servers* up and running at all times. For the majority of the Web, anyone anywhere is able to access the information someone has posted – at anytime. Some individuals choose to document their whole life on public web pages. Others have even provided the world an opportunity to view what happens inside of their homes in real-time via webcams. Many do not realize that once information flows over the Internet it gains three very important and potentially damaging characteristics of *persistence, transportability,* and *universality.*

Persistence is the understanding that the moment something passes over the Internet once, it can be assumed that someone, somewhere, has archived an exact electronic copy of that information – forever. Nor does it matter if the data is emailed or downloaded, encrypted or not. All information flowing over the Internet is first broken down into small parts by the sender. These 'packets' then look for and take the path of least resistance to their destination. Once at the other end, the packets are reassembled and checked for accuracy. A packet can travel around the world in a moment, passing through multiple nodes all over the world on its way to the final destination. As such, each packet is vulnerable to "packet sniffing" at every node through which it passes. Anyone can examine an unencrypted packet for its content. It is a safe assumption that

any Government whose judiciary will allow it has placed 'taps' on all nodes (ISPs) within its boundaries.[26] It is commonly understood that U.S. intelligence agencies currently employ a system known as "Echelon" which has the capability of monitoring all cellular, satellite, and a great deal of the ground based communications which pass through the U.S., Canada, the U.K., Australia, and New Zealand. It is also rumored that France, Russia, India, Pakistan, Israel and others are all employing similar capabilities.[27] One can imagine a small country with little technical or financial resources allowing an ally to 'tap' into its ISP(s) under a quid pro quo arrangement. Once an entity has allowed one intelligence agency to 'tap' its ISP there would be little stopping the entity from double-dipping and allowing yet other agencies from tapping the line a second or even third time. Given the assumption that the Internet has all kinds of ears to the wire, it would only be prudent for individuals and organizations to encrypt their more sensitive communications.

Even those with out access to an ISP and the software to conduct packet sniffing can benefit from a poor-man's version of *persistence*. One need only conduct a search using a popular web browser such as Google. Most users have noticed that nearly every return on a given search offers the option to view Google's "cache" of that site. In order to offer this function, Google archives an exact copy of a given web page. This is a common feature among search engines. Another more systematic example of *persistence* is that of the Internet Archive's "Waybackmachine" (www.archive.org) which provides a

---

[26]The U.S., the U.K., and Japan have all passed laws allowing police to require ISPs to provide information about users who are under investigation. In the U.S. the federal program is known as "carnivore" and enables federal agents with a subpoena to 'tap' the ISP if the ISP does not provide the information voluntarily. Robert Graham, *Carnivore Faq* [Internet] (2001 [cited 30 October 2004]); available from http://www.robertgraham.com/pubs/carnivore-faq.html.

[27]Ibid, Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: Wiley, 2000).

cache of most "surface web" sites posted since the mid-1990s. The "surface web" is the collection of static web pages that are catalogued by standard search engines.

While one cannot yet search the Waybackmachine for content, if the user has a target website, he can track the information which has appeared on its pages, and how that information has changed, over time. Savvy industry and government webmasters are aware of these archival sources and have successfully submitted the appropriate requests to have potentially harmful data expunged from the public archive. This does not mean that Google, Yahoo, Wayback, or anyone else has permanently deleted this data from *their* archives, however. It is not difficult to imagine that a Government with enough resources might find it well worth their while to imitate the capabilities of Google or the Wayback machine for their own 'in-house' use.

The average user is not limited to Google or the Wayback machine, however, in order to view long-since removed documents from the Internet. There exist numerous individuals and groups who, for various reasons, are wont to republish news articles, other peoples' web sites, and documents which have since been removed from government websites because of security concerns since 9/11. Two sites which typify this genre include the Federation of American Scientists (www.fas.org) and Global Security.org (www.globalsecurity.org). Users who do not have the resources of a well-endowed nation, but have a budget larger than that of the average user can purchase the work of professional open-source information gatherers. These organizations refine openly available information and turn it into useable intelligence.[28] Some excellent examples of this type of source include Military Periscope (www.periscope1.com), Janes

[28]This is a form of intelligence gathering which is termed OSINT (Open Source Intelligence) and will be discussed in detail during the next section of the paper.

Information Group (www.janes.com), and The Economist Intelligence Unit (www.EIU.com).

Transportability. Not too long ago, an 'insider' conducting espionage most often had to stay late, make photocopies, and carry bits of information out in a briefcase. Now an industrial or governmental spy can dock a miniature 80GB USB hard-drive to his work computer and download the equivalent of 3 million pages of information, undetected and unquestioned on many networks.[29] The following day the thief can repeat his actions in case he needs more. If the thief is sitting on the Internet backbone at a local university he can transfer the entire contents of his disk anywhere in the world in less time than it takes you to read this paper.[30] Furthermore the time lag between information collection and analysis could stretch from days to weeks. Today the analyst can be in a cave, underground bunker, or office building halfway across the world – or across the street. Distance and time are no longer a factor in the matter of information transportation.

The last characteristic of information is that of *universality*, or sharing everything with everyone – everywhere. Recent estimates cite the population of Internet users to be no less than 665 million users. It would be a mistake to assume that the over 167 Terabytes[31] of data indexed Google and other search engines are not combed daily for useful intelligence on a daily basis by potential adversaries across the globe.[32] While

---

[29]Calculations based on pure text files in .pdf format; 1MB = 45pp.

[30]Calculated using http://www.numion.com/Calculators/Time.html; 60Gig@ 622 Mbps (OC12) =12min 51sec.

[31]A Terabyte is one trillion bytes. The U.S. Library of Congress text holdings are estimated at 20 Terabytes. *Wikipedia*.

[32]*How Much Information?* [Internet] (University of California, Berkeley, 2003 [cited 20 April 2005]); available from http://www.sims.berkeley.edu/research/projects/how-much-info-2003/.

some sites might attempt to limit access from certain areas of the world through the technique of ISP-blocking, experienced users are able to bypass this relatively weak security measure.

2 – THEFT, WAR, & DIRTY TRICKS

Air Miles & Discount Cards

Identity theft is a growing problem in the United States. The Federal Trade Commission reported that in 2003 nearly 10 million Americans were victims of identity theft – a staggering 13% of the consumer population.[33] The costs of this increasingly common form of fraud are equally enormous. Banks and businesses lost over $48 billion and the average victim spent over 600 hours in order to restore their name.[34]

The list of culprits includes money launderers, drug smugglers, illegal immigration traffickers, as well as terrorists, and their job is getting easier.[35] These criminals are merely exploiting an increasingly 'target-rich' environment of online databases designed to store information on customers or potential customers. Recently, a large cell-phone provider reported that its extensive customer database had been compromised by a hacker over the period of seven months. The database contained the many of the most personal details about subscribers including photographs, text r

privacy policy of each information collector, this information may be sold outright. Even if the privacy policy is restrictive today, policies often change.

The immediate financial losses as noted above may only scratch the surface, however. Analysts are becoming concerned that the prevalence of identity theft is eroding consumer confidence in the Internet as a means of commerce. This erosion of trust is causing Americans to abandon, "online banking because of security concerns," and if left unchecked, this exodus could become a "trillion-dollar problem."[37]

Individual citizens are not the only ones worried about the safety and security of data stored on and passed over the Internet, however. The U.S. Government is very uneasy about the security of "cyberspace", or the online network of computers and infrastructure that comprise the Internet:

> Today, the cyber economy is the economy....virtually every vital service -- water supply, transportation, energy, banking and finance, telecommunications, public health...relies upon computers and the fiber-optic lines, switchers, and routers that connect them. Corrupt those networks and you disrupt the nation. It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating -- also makes us more vulnerable.... – Condoleezza Rice[38]

Ms. Rice has significant reason to be alarmed. We are, perhaps more than any other country in the world, a nation dependent on the Internet.

Network Malfunction

One author describes the threat embodied in the potential "blowback" effects of our reliance on the Internet. Many are now concerned that one critical point of failure

---

[37]Ibid.

[38]Condoleezza Rice, *U.S. Security Policy: Protecting the Nation's Critical Infrastructure* [Internet] (U.S. Department of State, 2005 [cited 20 April 2005]); available from http://usinfo.state.gov/journals/itps/0301/ijpe/pj61rice.htm.

could bring down the whole network.[39] We have become increasingly dependent on "complex software that is at best imperfectly understood, and whose failures are difficult to predict. Components fail, accidents occur and sabotage can happen."[40] The term for this complex interaction is sometimes called, "network interdependency".[41]

More disconcerting is the possibility that the critical point of failure may, in fact, be *outside* of national boundaries given the nature of our reliance on a just-in-time supply network consisting of global companies. Now, "governments and companies have found it almost impossible to map and understand their wider dependencies."[42] A former Japanese cabinet minister, speaking about Japanese manufactured microprocessors used in U.S. missile guidance systems, pondered aloud, "if Japan stopped selling [the U.S.] chips…there would be nothing more they could do…this would upset the entire military balance."[43]

The global network of uncharted interdependencies goes far deeper than vulnerabilities within our defense infrastructure, however. This network affects every facet of every American life. The malfunction of any part of the national infrastructure "can have a significant impact on the physical and economic well-being of a country and its people."[44] One such example occurred in the United Kingdom in September of 2000.

---

[39]Andrew Rathmell, *Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations* [Internet] (RAND Europe, 2001 [cited 20 April 2005]); available from http://www.nato.int/acad/fellow/99-01/rathmell.pdf, 22.

[40]Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Critical Infrastructures against Cyber-Attack*, trans. 359: 1 (New York: Oxford University Press, 2003), 5.

[41]Rathmell, *Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations*, 22.

[42]Ibid.

[43]Toffler and Toffler, *Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, 425.

[44]Lukasik, Goodman, and Longhurst, *Protecting Critical Infrastructures against Cyber-Attack*, 5.

Over the course of six days, protesters at an 11 British oil refineries effectively created a nationwide fuel shortage by blocking trucks from transporting their cargo. This resulted in panic stricken consumers rushing to grocery stores to purchase staple items. Banks ran out of cash, the Royal Mail, bus and train services nearly came to a stop. Aircraft were forced to reroute to one of two airports serviced by private pipelines and the Confederation of British Industry gave notice that they would no longer be able to continue production due to shortages. The protesters finally withdrew, but not before causing an estimated $1.4 billion in damages to the British economy.[45] This example shows how vulnerable our modern networks can be to critical points of failure. The following sections describe some of the methods and the characteristics of those whose intent is to cause and exploit failures.

The significance of network interdependences and associated weaknesses created by the information revolution has not been lost on our potential adversaries. The new environment provides ideal platforms for asymmetric attack by both terrorists and peer competitors who cannot with the U.S. on the old-fashioned battlefield. Much of the current literature seems unduly focused on eliminating the terrorist threat perhaps at the expense of a more ominous and potent threat.

Nearly six years ago two Chinese military officers penned the book, Unrestricted Warfare. In it they describe a set of "new-concept weapons" which could create a man-made stock market crash. The writers speak of an environment where the *old* rules are no longer in effect and a battlefield where "visible national boundaries, invisible Internet space, international law, national law, behavioral norms, and ethical principles, have

---

[45]Ibid., 10.

absolutely no restraining effects…"[46] The authors predict that "…people will awake to discover with surprise that quite a few gentle and kind things have begun to have offensive and lethal characteristics…blurring…the concept of who the war participants are."[47] In this form of warfare, the attacker will defeat its opponent by

> …secretly muster[ing] large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.[48]

This proposed doctrine should be taken seriously in light of China's recent mustering of several battalion-sized units capable of conducting cyber-warfare.[49]

Bad Guys

Potential attackers range from organized crime, hackers or hacktivists, virus writers, malicious insiders, or information warfare by both state and non-state actors.[50] Both the motivations and capabilities of the categories differ greatly. Some are joyriders, others deeply intent on causing damage or conducting international espionage. The U.S. Department of Defense uses a tiered system to help describe the variety of capabilities and resources that exist.[51]

---

[46]Qiao Liang and Wang Xiangsui, *Unrestriced Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 132.

[47]Ibid., 25-26, 48.

[48]Ibid., 145-46.

[49]Timothy L. Thomas, "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice," (Fort Leavenworth, KS: Foreign Military Studies Office, n.d.).

[50]James M. Jenkins, "Computer Network Defense: DoD and the National Response" (Air War College, 2002), 14.; Schneier, *Secrets and Lies: Digital Security in a Networked World*, 42-58.

[51]*FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 1-4.

- **Level 1**. "Lone or small groups of amateurs using common hacker tools and techniques in an unsophisticated manner without significant support."
- **Level 2**. "Individuals or small groups supported by commercial business entities, criminal syndicates, or other transnational groups using common hacker tools in a sophisticated manner. This level of adversary includes terrorists and nongovernmental terrorist organizations. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft."
- **Level 3**. "Individuals or small groups supported by state-sponsored institutions (military or civilian) and significant resources, using sophisticated tools. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft."
- **Level 4**. "State-sponsored offensive IO, especially computer network attacks (CNAs), using state-of-the-art tools and covert techniques conducted in coordination with military operations."

This construct is useful for understanding the range of actors that might attack a system, but in order to gain a better appreciation of the threat we must also understand some of the various techniques currently used by opponents. These techniques can be broadly categorized as either *passive* or *aggressive*. The first category is often exploited during the intelligence-gathering portion of an attack and can last from days to years based on the patience and sophistication of the attacker. The second category can be used either to aid in intelligence gathering or may be used as a means of attack.

Libraries, cookies, and espionage

The Internet by its very nature was designed to be an open environment where anyone could instantly share just about any information with anyone else, anywhere, at anytime. It is somewhat ironic that the nation that first led the establishment of the Internet now faces some of the greatest threats from it.[52] Any information that travels the Internet is subject to exploitation by foreign powers, both state and sub-state. In the heyday of the Internet revolution in the mid-1990s many American institutions both public and private rushed to put as much information on the Internet with seemingly little thought to the possibility of potential exploitation. As the Internet has matured, so have organizational policies towards information to be posted on the Internet. Even so, information continues to appear on the Internet that could be damaging to the national security of the United States. One of the first governmental agencies to show concern for these happenings was the U.S. Department of Defense (DoD). Though not the first instruction regarding web security, one of the most comprehensive directives issued by the DoD was published in September of 1998. The policy memorandum entitled, "Information Vulnerability and the World Wide Web" emphasized the positive aspect of the Internet as an essential conduit of information to the American citizenry, but warned that information posted thereon might violate operational security (OPSEC).[53] Therefore, the memo directed that all elements of the DoD conduct a review of their websites,

> …ensuring that the information published on those sites does not compromise national security or place DoD personnel at risk…Component heads must enforce the application of comprehensive risk management procedures to ensure that the considerable mission benefits gained by using the

---

[52]Prashant Bashki, "Open Source Intelligence: A 'Force Multiplier'," in *NATO Open Source Intelligence Reader* (NATO, 2002), 95.

[53]*Information Vulnerability and the World Wide Web* [Internet] (Department of Defense, 1998 [cited 5 Feb 2005]); available from http://www.defenselink.mil/other_info/depsecweb.pdf.

> Web are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audience.[54]

Three years later the entire federal government followed suit with its own guidance. In March of 2001 a White House memo was issued to the heads of all federal departments and agencies ordering "an immediate reexamination" of measures for identifying and protecting information on WMD and "other information that could be misused to harm the security of our nation and the safety of our people".[55] Seven months later, shortly after the infamous attack on the twin towers, the Department of Justice informed all federal agencies that the prudent removal of any Freedom of Information Act (FOIA) information from the public eye would be fully supported by the Department of Justice (DoJ).[56] Another three months after that, the Director of the Office of Public Security issued guidance to all agency heads to review and remove all "sensitive" information from their websites.[57]

Due to the prevalence of the WWW, one of the cheapest and most effective means of intelligence collection today now comes from open-source intelligence (OSINT) gathered from the web. OSINT is defined as:

> …publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROMs. It may be disseminated to a broad public, as are the ma

There are undoubtedly vast amounts of OSINT information still in traditional formats, but increasingly paper, film, and magnetic media are being digitized and posted on the web. Even *grey literature* such as broadcast radio, television, telephone directories, and maps are increasingly available from the Internet. Every day archivists digitize more and more information. Academic journals and conference proceedings are being systematically electronically archived and made accessible by most large universities through subscription database services such as www.jstor.org, and www.ebsco.org. Some university libraries are in the process of digitizing the sum of their holdings and Google currently offers a beta version of a scholarly literature search engine through its www.scholar.google.com website.[59] Www.amazon.com offers a "Search Inside the Book" feature which allows the user to search for a specific word or phrase as it might appear in one of the millions of pages which Amazon.com has archived electronically. Reports state that Amazon.com plans to enable this feature for every book it sells.[60] Meanwhile, Google is in the process of archiving the holdings of five major University libraries.[61] It is conceivable that the sum of written knowledge will be available online within a matter of years.[62]

It is notable that some of these sites are not as easily searchable as others since they belong to a realm of the Internet known as the "deep web" where data is indexed through a complex dynamic database rather than persistent links. It is unlikely for a user

---

[59]Carolyn Said, *Revolutionary Chapter Google's Ambitious Book-Scanning Plan Seen as Key Shift in Paper-Based Culture* (December 20 2004 [cited 20 April 2005]); available from http://www.sfgate.com/cgi-bin/.

[60]Gary Wolf, *The Great Library of Amazonia* [Internet] (2003 [cited 20 April 2005]); available from http://www.wired.com/news/business/0,1367,60948,00.html.

[61]Said, *Revolutionary Chapter Google's Ambitious Book-Scanning Plan Seen as Key Shift in Paper-Based Culture*.

[62]For a fee, of course; much like the academic databases of today charge for content.

to stumble upon information in the "deep web" unless he/she is visiting a website and types the correct search term on the target site. In other words, you won't get results for these websites on Google…yet. In 2002 the estimated quantity of data on the "surface web" was 167 terabytes while the "deep web" was thought to contain over 90,000 terabytes of data. Not only vastly larger, the "deep web" contains information that is of much higher quality than its little brother.[63] This means that vast quantities of information are available to those who search for it, and it will only become easier to find OSINT intelligence on the web – making defense of the homeland all the more difficult.

Another more subtle form of information gathering is found in the maturing art of "web analytics".[64] Web analytics is the process by which intelligence (both corporate and national) are able to gain critical information about their targets by observing their Internet usage habits. Through the usage of 'cookies' websites are able to monitor a computer user's historical Internet usage and analyze patterns. Companies such as DoubleClick specialize in aggregating customer data from disparate websites.[65] Once collected and analyzed this data can be correlated with email accounts and individuals can be targeted based on their Internet browsing habits. After having compiled a highly detailed composite of a given user's buying, surfing, sleeping (what time did they log off?), and even eating habits (did they order their takeout online?), companies like DoubleClick are free to sell this information to anyone. The Markle Foundation counts nearly 150 databases that contain personal information from library borrowing habits to credit card transaction reports. Fully one-third of the databases are either available for

---

[63] *How Much Information?*.

[64] *Protecting Corporations from Internet Counter-Intelligence* [Internet] (Anonymizer, n.d. [cited 16 April 2005]); available from http://www.anonymizer.com/enterprise/info/papers.shtml.

[65] Schneier, *Secrets and Lies: Digital Security in a Networked World*, 171.

research to anyone with a small fee, or in some case entirely free.[66] Who is purchasing this information? While privacy advocates are concerned with big brother, these databases may also be used by stalkers or a foreign intelligence agency looking for someone with an exploitable weakness.

Another element of web analytics is IP-based analysis, through which corporations and governments may glean information inadvertently leaked through routine Internet usage. This can be as simple as a search engine that suddenly gets a spike in search requests for the terms "Sudan" and "infrastructure" from an ISP serving Tampa, Florida – indicating that CENTCOM may be considering military action in Sudan. Depending with whom the search engine company is allied this could constitute a significant compromise for an operation that has not even begun. In the corporate world this type of breach of OPSEC can lead to significant economic losses. In one case, employees from one company, while researching for the hostile takeover of another company left traces of their (OSINT) investigative web surfing on the target company's web server. The target company, noting numerous hits coming from the competitor's IP address, especially on certain web pages dealing with profits and losses, deduced that a takeover was in the works and was able to creatively manipulate the bidding process to *its* advantage.[67] Assisting web-analytics are cookies that can track a user's browsing habits as well as the site from which the user just came. If a user happens to browse the Sudanese Minister of the Interior immediately after viewing the internal directory,

---

[66] *Creating a Trusted Network for Homeland Security* [Internet] (Markel Foundation, 2003 [cited 20 April 2005]); available from http://www.markle.org/.

[67] *Protecting Corporations from Internet Counter-Intelligence.*

"c:/sudan/OPORD_0506" he has unwittingly provided critical information to the Sudanese government.[68]

Web site hosts may also selectively block or change what information the requestor sees based on the requestor's IP address. Using "IP-based blocking" and "IP-based cloaking", respectively, web administrators may either deny a request (block), or more subtly, change (cloak) the content to suit the requestor's IP address. Company A may display inflated product prices to all requests emanating from company B's IP address. If company B acts on this (false) information and prices their goods comparably, they will find themselves with few customers. Recently, "a well-known Arab news service" distributed different editorial pages to requestors from Western-based IPs than it did requestors from Middle-Eastern IPs. The Westerners received a western friendly version while the others received "anti-Western, anti-Israel, and anti-Semitic views."[69]

Another source of Internet information that is worthy of special mention is the availability of remote sensing/satellite photography to anyone with a credit card and an Internet connection. This one aspect of the information age has changed the nature of national security in that data previously the sole purview of world superpowers can now be had by individuals for a small fee, and in some cases for free.[70] This has been a windfall of for both state and non-state actors. With only the use of information openly

---

[68]It would be a major breach of security for anyone to use a computer on the Internet that also has access to classified documents, but this type of breach *has* occurred in private industry where the stakes are quite high. Ibid.

[69]Ibid.

[70]Beth E. Lachman John Baker, David R. Frelinger, Kevin M. O'Connell, Alexander C. Hou, Michael S. Tseng, David Orlosky, Charles Yost, "Mapping the Risks: Assessing Homeland Security Implications of Publicly Available Geospatial Information," (Pittsburgh, PA: RAND Corporation, 2004), 20.

available on the Internet, adversaries can inexpensively and remotely meet many of their intelligence requirements in planning a future attack. The following section describes some of the most popular techniques currently used to conduct CNA and CNE against networks.

Shoulder-surfing & Spying Trojans

All CNA and CNE operations are best understood as the effort by one party to increase his relative power while causing his opponent to lose power. This principle applies to both the military and industrial context. Sometimes this is accomplished by stealing data (espionage) in order to enhance one's competitive advantage in the marketplace. Other times the attacker may find greater advantage in disrupting his adversary's networks by corrupting or even destroying the competitor's data. An attacker may also seek the use of a third party's network in order to mask the true origin of the attack or to mass greater computing power against the eventual target. Whatever the method of attack, the tools used are often the same.

In order for malicious agents to gain entry onto a system they must first gain access to the target system. One of the most effective means of gaining access to even the most secure of systems is through what has been termed, "social engineering." Author and reformed hacker/social engineer Kevin Mitnick describes various techniques that can be employed to effect a successful attack in his book, "The Art of Deception."[71] Even the most secure of systems are dependent on humans, and many security experts contend that humans will always be the weakest link in a technologically well-secured

[71]William L. Simon Kevin D. Mitnick, Steve Wozniak, *The Art of Deception: Controlling the Human Element of Security* (Wiley, 2002).

environment.[72] This should not be used as an excuse to abandon technical security measures; rather it should serve as a warning to those who believe technology alone can save networks from malicious agents. One of the simplest forms of password attack is called, "shoulder surfing" – that is surreptitious observation of the target as they enter their user ID and password. Some of the approaches to compromising an adversary's computer system are purely technical while others rely to varying degrees on an unwitting ally who can give access to the network. The following paragraphs will provide a brief overview of the existing terrain of malware.

Viruses are the original malware. They spread after attaching themselves to a piece of software or file that is transferred from one computer to another. Sometimes the term "virus" is used mistakenly to refer to other types of malware. Worms are similar to viruses but do not require a host file in order to spread. Instead they are able to self-propagate. In the past, worms and viruses have caused a great deal of damage by disrupting networks and the flow of data. As popular operating systems have begun to allow greater functionality through third party software 'plug-ins', a new breed of malware has become increasingly prevalent. This includes the now infamous spyware and its cousin the Trojan horse. Spyware and Trojans are very similar in form and function, both requiring the user to download a harmful piece of software. The most basic forms of spyware can attach themselves to a user's machine without any input from the user if the operating system or one of its applications has a security flaw. The user is usually unaware of the parasite until they realize that their system has slowed to a crawl. These programs can report the user's browsing habits and more. More harmful forms of

---

[72]Ibid, Schneier, *Secrets and Lies: Digital Security in a Networked World*.

spyware are essentially Trojans, requiring user complicity to gain access. This can be as easy as clicking "OK" or yes to one of the hundreds of dialogue boxes a user encounters on a weekly basis, or coercing a user into downloading it by claiming that content on the page will not display properly until this piece of software has been installed.[73] Once a Trojan has gained access, even the most sophisticated users may remain unaware of its presence. Many Trojans can intercept user IDs and passwords using keystroke-logging software, later sending the information back over the Internet to a malicious actor.[74]

Once installed, spyware and Trojans are notoriously difficult to remove. New methods of malware implementation appear daily. One recent means involves the malicious software burrowing itself deep into the kernel (fundamental structure) of the operating system. This attack is described as being "almost impossible to detect using current security products." The complexity of this type of attack is reflected in the tone of a statement by a senior member of the Microsoft Security Solutions Group, "these people are smart, very smart."[75]

---

[73]"Do you wish to trust content from XXXX?" A good answer is "no."

[74]*Wikipedia*. Though not spyware, another similar vulnerability worth noting is that of the ability to monitor the last item stored in the user's 'clipboard' using Microsoft's browser, Internet Explorer. Many users increasingly use the clipboard to transfer ('cut and paste') one of their many passwords from a file to the browser. A well-versed webmaster can include script that allows him to download the last piece of data on the user's clipboard as long as the browser settings are at their default level. Not considered a security threat by the browser manufacturer, a user must manually change the settings to prevent information leakage: Tools > Internet Options > Security > Select a security zone > Custom Level > Scripting > Allow paste operations via script > Disable or Prompt. For more information on this see: Tom Gilder, *IE Clipboard Stealing Vulnerability* [Internet] (! [cited 25 April 2005]); available from http://tom.me.uk/clipboard/.

[75]This type of attack is called a "rootkit" since it installs on the system root or kernel. See: Paul Roberts, *Microsoft Warns of New Security Threat: System Monitoring Programs, Called Rootkits, May Pose a Serious Danger to Your Pc.* [Internet] (PC World, 2005 [cited 25 April 2005]); available from http://www.pcworld.com/resource/article/0,aid,119720,pg,1,RSS,RSS,00.asp.

Yet another threat is that of browser hijacking, or URL hacking.[76] This can range from annoying – being constantly redirected to a site that the user did not request, to extremely compromising. Two examples of the latter are called phishing and pharming. Phishing is usually initiated by an email that appears to be from a trusted agency (such as the user's bank) requesting that they log on. Once the user clicks on the link in the email he is redirected to a site that appears exactly like the banks online site except it isn't. From there the malicious agent collects the user's ID and password and in turn often delivers an error message to the effect of, "web site temporarily not available – try again later." Pharming is similar, except in this case the agent conducts a high level attack against the domain name server (DNS) – the agency which ensures the letters "www.usersbank.com" are translated into an IP address. Instead of being directed toward the user's bank site he is directed again toward that of a malicious agent.[77] Both Phishing and Pharming lend themselves to the more complex "man-in-the middle" attack where the attacker acts as a relay point between both connection points – making his presence invisible while monitoring even encrypted traffic.[78]

Depending on its purpose, malicious code can present itself as merely a nuisance (e.g. turning a computer off at random intervals, changing screen settings, or displaying a message) to transforming the attacked computer into a host for a larger "botnet". A *botnet* is a network of compromised computers that responds to the will of an outside

---

[76]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 168, *Wikipedia*.

[77]*Wikipedia*.

[78]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 114.

agent – someone who could be halfway around the world.[79] *Botnets* give the controlling individual or agency access to incredible computing power that could be used for purposes such as cracking passwords and encryption to levying a massive distributed denial of service (DDOS) attack such as occurred in 2002.[80]

The chief reason for the increasing prevalence of "patches" to fix security holes is a function of both user demand for ever-increasing "functionality" as well as software creators' desire to fulfill our demands with the cheapest alternative possible. The first element to be sacrificed is that which is least visible to the user: security.[81] This is evident both in the design of some of the most popular Operating Systems (OS) as well as many popular software applications.

Every operating system such as Microsoft Windows or Linux is based on a core piece of code called a *kernel*. The greater the complexity of the *kernel*, the more likely it is that it will have exploitable features. If the *kernel* is exploitable, any security piled on top of it is useless – a one hundred character password changed hourly offers no protection against this shortcoming.[82] Microsoft Windows is known for its particularly 'functional' but cumbersome *kernel* and Microsoft is constantly churning out "patches" to fix the exploitable problems in its *kernel*.

Modern application software (word processing programs, games, and anything else that runs on an OS) offers extraordinary flexibility. A user of Microsoft Word can

---

[79]Individual machines are sometimes called "zombie" computers. A friendly form of the *botnet* is found in examples such as SETI (Search for Extra-terrestrial Intelligence) and the EFF (Electronic Freedom Foundation) network of computers used to crack the U.S. Government's "unencryptable" DES algorithm.

[80]Bradley K. Ashley, *Anatomy of Cyberterrorism: Is America Vulnerable?* [Internet] (Air War College, 2003 [cited 30 October 2004]); available from www.au.af.mil/au/awc/awcgate/awc/ashley.pdf, 20.

[81]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 359-60.

[82]Ibid., 128-29.

create a custom program (or "macro") to perform just about any task imaginable. While the typical user never uses this functionality, a skilled programmer can manipulate these tools to create malicious code that can compromise the entire network.

A recent survey of home computers found 80% of all computers were infected with some form of spyware.[83] This figure does not just represent an annoyance that can be swept away by better legislation and enforcement, but rather an indication that we as a networked nation are increasingly vulnerable to attack. Networks—personal, business, and government—penetrated by malware may be not just be sending information to prying marketers but also to industrial and governmental spy agencies. There is little reason for them not to attempt to do so.

One might be tempted to think that the security of a corporation X's computer network is of minimal importance to national security, or that grandma's PC on the back porch is of no importance to the security of the nation. A network's security is dependent upon the security of its individual members. If a malicious agent is able to create a botnet of hijacked machines, he is able to harness enormous computing power to conduct a targeted Denial of Service attack against a critical portion of any network. He can also use these machines to mask his identity, location, store files or conduct complex calculations. Stolen money and identities can be used to help finance and outfit terrorist organizations. Moreover, a trusted employee who periodically works from his home computer—which has been compromised by a Trojan his son downloaded— potentially compromises the entire network.

---

[83]AOL/NCSA, "AOL/NCSA Online Safety Study," (America Online & National Cyber Security Alliance, 2004), 4.

SCADA-logical

The systems most critical to our nation's infrastructure have been designated as SCADA (Supervisory Control and Data Acquisition) systems. SCADA systems "perform key function[s] in providing essential services and commodities (e.g. electricity, natural gas, gasoline, water, waste treatment, transportation) to all Americans."[84] The U.S. government has placed a great deal of effort into its attempt to secure SCADA networks in recent years, due to the dual realizations after 9/11 that adversaries did indeed exist and that much of the information regarding the operation of these networks was -0.0033 Tw 12 0 0 12 89.99991 496.67981 Tm-0.00T542o 02fe09 575384as

corporations, local, state and federal governments.[89] In the last decade numerous attacks on these and other systems have been made public with others likely occurring, but remaining unpublished so as to prevent widespread panic.[90] Some notable examples include the breach of an Arizona water and an electricity provider's computer system, the computerized release of a 264,000 gallons of raw sewage, an attack against the control systems of a power production and transmission facility in California, and more recently, the revelation that the 2003 SQL Slammer worm had disabled the safety monitoring system at nuclear power plant.[91]

---

[89]Ibid.

[90]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 391-92.; An analogy to this concept is fate of CITIBANK in 1995 after it publicized the details of a $12 million hacker theft and its corrective security measures. Customers responded by withdrawing millions of dollars, significantly reducing bank reserves. In the public sector, the revelation of a successful attack against U.S. government infrastructure computers could similarly result in a drop in the value of the dollar.

[91]Dacey, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," 17.

3 – DEFENDING THE "NET"-NATION

The Average "Joe"

Most individual Internet users have little to no idea how they and their information can be compromised online. Despite assurances given by the little gold padlock on a user's Internet browser, IA is not a reality for the average citizen. While the chances of being the victim of exploitation are significantly reduced by taking prudent measures such as using a regularly updated anti-virus program, incorporating hardware and software firewalls, and regularly downloading operating system critical updates, a determined attacker can still compromise any system connected to the Internet.[92] This is demonstrated clearly through the number of average home computers are not adequately protected against viruses (67%) and are infected with spyware (80%).[93]

Corporate Defense

Currently many large corporations and government agencies are spending enormous amounts of money to ensure that their systems are secure enough to meet their own risk-benefits analysis. That is to say, corporations (and government) will weigh the return on investment (ROI) for a given security measure.[94] If a corporation must pay more to implement appropriate security measures than it would cost to rectify the associated breach it makes little business sense for the organization to spend more money on preparing for something that would cost less to repair after the damage is done. For the most part this means that corporate security is at a much higher level than that of the average home user. Most corporations have a dedicated Information Technology (IT)

---

[92]In this case he may have to revert to a combination of *dumpster diving* and *social engineering*.

[93]AOL/NCSA, "AOL/NCSA Online Safety Study."

[94]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 301.

staff whose fulltime job is to ensure that the network is protected against viruses and malware through strict policies and regular systems updates.

Furthermore, big businesses recognize the threat of industrial espionage and many have taken the initiative to provide employees with the means to encrypt as well as digitally sign communications. Modern encryption techniques have evolved considerably since the German's fielded the "Enigma" machine. While some foundational principles remain the same, new techniques have evolved over the last half-century. One of the most significant steps was the introduction of "public-key" cryptography in 1976.[95] A public key infrastructure, or PKI allows for both the possibility of digital signatures and encryption. Digital signatures allow for the possibility of "non-repudiation" or inability to deny that one sent a signed email, for instance. Encryption allows for confidential communication between individuals. The following is a simplified description of how Alice uses public-key (PKI) to encrypt a message:

> Alice wishes to send a secret message to Bob…she looks up Bob's public key in a directory, uses it to encrypt the message and sends it off. Bob then uses his private key to decrypt the message and read it. No one listening in can decrypt the message. Anyone can send an encrypted message to Bob, but only Bob can read it (because only Bob knows Bob's private key).[96]

And how Alice can digitally sign a document:

> Alice does a computation involving both her private key and the message itself. The output is called a digital signature and is attached to the message. To verify the signature, Bob does a computation involving the message, the purported signature, and Alice's public key. If the result is correct according to a simple, prescribed mathematical relation, the signature is verified to be genuine; otherwise, the signature is fraudulent, or the message may have been altered.[97]

---

[95] *What Is Public-Key Cryptography?* [Internet] (RSA Laboratories, n.d. [cited 29 March 2005]); available from http://www.rsasecurity.com/rsalabs/node.asp?id=2165.

[96] Ibid.

[97] Ibid.

Government Approach

In order to conduct the attacks described in the preceding section, an adversary must have information. In fact, in order to launch *any* type of successful attack, an attacker must conduct reconnaissance and assessment. In western military doctrine this is known as Intelligence Preparation of the Battlefield (IPB) which is:

> …an analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process.[98]

Skilled adversaries will structure their attacks against a given target by first exploiting openly available information to help select the target; exploit open source information pertaining to the target system and its vulnerabilities; conduct rehearsals against mockups of the target system. Finally, once complete with rehearsals, the attacker can mount his attack at the time of his choosing – with lightning speed.[99]

The critical element to the intelligence preparation (IPB) phase of the attack is access to information. Information is critical to target selection as well as a refined detailed assessment of the target's vulnerabilities. Ironically, the Internet has provided and continues to provide attackers with the tools to conduct IPB on a variety of targets in the U.S. A senior defense official has affirmed that that al Qaeda training manual states that, "using public sources openly and without resorting to illegal means, it is possible to

---

[98]*JP 1-02: Department of Defense Dictionary of Military and Associated Terms* [Internet] (Department of Defense, 30 November 2004 2001 [cited 25 March 2005]); available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[99]Lukasik, Goodman, and Longhurst, *Protecting Critical Infrastructures against Cyber-Attack*, 12.

gather at least 80 percent of all information required about the enemy."[100] One author has termed this use of the Internet by terrorists, "cyberplanning." [101]

To date, however, governmental policy has been less than aggressive in this area. In the recently published National Security to Secure Cyberspace (NSSC) the government response largely ignores the private sector and its role in securing information systems. Instead, the government exhorts the reader to remember that, "all users of cyberspace have some responsibility, not just for their own security, but also for the health of cyberspace." [102] While this might work as an encouragement for a group of concerned citizens to pick up trash around the neighborhood, it is unlikely to be effective in an environment where the average user is as ill prepared to fend off cyber threats as a lost sheep might be thwarting the attack of a pack of wolves. As one author puts it,

> The current U.S. strategy for cyber security is based on a presumption that everyone who owns and operates a computer or a network of computers is responsible for ensuring they protect themselves against an attack. But in reality, when skilled and professional hackers, cyber terrorists, or state sponsored operators, are aggressively attempting to invade one's privacy, individual users are not typically educated or prepared for this challenge.[103]

Instead of providing proscriptive guidance to industry, the NSSC offers a proposal creating, "voluntary partnerships among government, industry academia, and

---

[100]Gabriel Weimann, *www,terror.net: How Modern Terrorism Uses the Internet* [Internet] (United States Institute of Peace, 2004 [cited 30 Oct 2004]); available from http://www.usip.org/pubs/specialreports/sr116.pdf, 7.

[101]Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of "Cyberplanning"," *Parameters*, no. Spring (2003): 113.

[102]Benoît Gagnon, *Are We Headed for a "Cyber-9/11?": The Failure of American Cyberstrategy* [Internet] (Raoul-Dandurand Chair Website, 2004 [cited 21 April 2005]); available from http://www.dandurand.uqam.ca/download/pdf/isa2004/gagnonb.pdf.; George W. Bush, *The National Strategy to Secure Cyberspace* [Internet] (2003 [cited 2004]); available from http://www.whitehouse.gov/pcipb/, 37.

[103]Timothy O'Hara, "Department of Homeland Security Policy for Defense of Cyberspace" (U.S. Army War College, 2003), 15.

nongovernmental groups to secure and defend cyberspace".[104] One author sums up the value of the NSSC by calling it a "paper tiger, lacking any statute authority."[105] In short, the NSSC seems to be a well intentioned, but misguided document. The focus appears to be solely on the threat of terrorism, wholly disregarding the possibility of an attack by a competitor state.

As a result of the increasingly complex interdependencies between the private sector, government, and national security, the lack of cooperation between government and industry apparent in this high-level document is particularly troubling:

> Although the history of technological change has always been somewhat chaotic, the change itself has seldom, if ever been so rapid and far-reaching. Thus, the importance of foresight and government-industry cooperation is crucial. Otherwise, the tremendous opportunities offered by information technology in general and such things as the Internet may actually lead to increase[ed] use of isolated networks and specialized, unique, an non-interoperable solutions and applications – or we will forego security altogether."[106]

Not sharing information with the right people deliberately discards the advantages conferred by the information age. The next section discusses one possible solution to rectify the current state of affairs.

As stated earlier, the DoD recognized the OPSEC threat posed by information published on the WWW and implemented an agency-wide review in 1998.[107] Even so, it was only after the events of September 11th, 2001 that many government websites began removing potentially exploitable information in earnest. The twin revelations that foreign agents might want to attack our homeland and that they could use the Internet to help them plan and execute the attack served to emphasize the power of information. Al

---

[104]Bush, *The National Strategy to Secure Cyberspace*, 2.

[105]Jenkins, "Computer Network Defense: DoD and the National Response", 25-26.

[106]Dennis D Steinauer, Shirley M. Radack, and Stuart W. Katzke, *U.S. Government Activities to Protect the Information Infrastructure* [Internet] (U.S. National Institute of Standards and Technology, 1997 [cited 20 April 2005]); available from http://csrc.nist.gov/publications/secpubs/, 22.

[107]*Information Vulnerability and the World Wide Web*.

Qaeda and other terrorist organizations are known to use the Internet and computer technology to plan, distribute of propaganda, recruit, train, fundraise, and even command and control agents in the field using anonymous email accounts and encrypted messaging.[108] The result of the 9/11 attacks was the wholesale reduction in availability of potentially sensitive governmental information on the web.

A sampling of data which have been lost include: reports on chemical site security and acceptable chemical exposure levels; geospatial data and statistics relating to transportation routes and pipelines; detailed maps and descriptions of nuclear, energy, and chemical facilities; risk management plans; data pertaining to the enforcement of aviation regulations; reports on water resources; various National Archive and Records Administration data; and data from the Internal Revenue Service.[109] This list is by no means exhaustive in that it does not include data published by non-federal governmental sources (state, local, and private industry). No list will ever capture the full magnitude of what has been removed since a great deal of this information was in the domain of the "deep web" and is by definition extremely difficult to catalogue. Further complicating research into the matter is the fact that publicly available Internet archives (e.g. www.archive.org, various search engines) have removed these pages.

"Classifying" the unclassified…

The U.S. government categorizes information as either *classified* or *unclassified*. *Classified* information is that information which in the interests of national security "has

---

[108]Weimann, *www,terror.net: How Modern Terrorism Uses the Internet*.

[109]"Access to Government Information Post September 11th."

been determined to require…protection against unauthorized disclosure."[110] Classified information is further categorized as, Confidential, Secret, or Top Secret.[111] With the explosion in availability and transportability of information in the wake of the information revolution, however, concern is growing that even unclassified information can now be easily aggregated to create a product which would otherwise be classified. A recent example of how extensively unclassified information can be aggregated is William Arkin's recent book, "Code Names" which, after years of compilation, gives an overview of thousands of classified programs whose very names are not to be uttered in public by those sworn to secrecy.[112]

As a result of the information revolution and the ease with which information may be distributed and analyzed with increasingly sophisticated software, the U.S. Government has removed information from its websites that could be used maliciously. In order to prevent itself from revealing this information via FOIA requests, more and more documents are beginning to fall under a subcategory of information that while not classified is considered "sensitive." One criterion for such data is any information that could aid in the creation of weapons of mass destruction (WMD) or could easily be aggregated with other unclassified data to create potentially damaging intelligence.

The current situation is relatively incoherent, however, with different agencies each creating its own definition of sensitive information. To confuse the matter further, it

---

[110] *JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

[111] *DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements* (v 1.2) [Internet] (Defense Informations Systems Agency, 19 March 1999 [cited April 20 2005]); available from www.fas.org/sgp/othergov/dod/genser.pdf.

[112] William Arkin, *Code Names: Deciphering U.S. Military Plans, Programs and Operations in the 9/11 World* (Hanover, NH: Steerforth Press, 2005). Arkin is another frequent republisher of information that the U.S. government would prefer not be published, yet Arkin sees himself as a patriot, giving citizens insight into what he feels are overly-classified government operations.

is not uncommon to see one agency's marking used by another agency which has its own marking for the same category. The Department of State uses the Sensitive But Unclassified (SBU), the Department of Defense the For Official Use Only (FOUO) marking. The Drug Enforcement Agency has claim to the DEA Sensitive marking.[113] DoD Unclassified Controlled Nuclear Information (DoD UCNI) is to be handled in nearly the same manner as classified information – but it is still considered unclassified.[114] The Department of Energy uses Sensitive Unclassified Information as its moniker for less-than-secret information, and the DoD labels some of its more sensitive field manuals with the marking, Distribution Restriction, "Destroy by any method [to] prevent disclosure of contents or reconstruction of the document."[115] The Department of State has authored the Limited Distribution (LIMDIS) marking which also shows up on some National Geospatial-Intelligence Agency (NGA) materials.[116] The Transportation Security Administration (TSA) has Sensitive Security Information (SSI), and the DoD super category for the those items bearing the marking SBU, DoD UCNI, and "Sensitive Information" fall under the general term: Unclassified Controlled Information.[117] A

---

[113]*DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements*.

[114]Alice R. Buchalter, John Gibbs, and Marieke Lewis, *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information* [Internet] (Federal Research Division, Library of Congress, 2004 [cited 27 April 2005]); available from http://www.fas.org/sgp/library/sbu.pdf, 15, 16.

[115]https://akocomm.us.army.mil/usapa/doctrine/

[116]*DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements*.

[117]In all cases the intent is to prevent sensitive information from falling into the wrong hands. In some instances material unclassified in a manner below may be an attempt to hide information which should be in the open. In other cases, such as that of DoD UNCI, the handling procedures for data so classified is remarkable similar to that of SECRET data, one can hardly help wondering if the DoD is unable to gain clearances (lack of time and/or money) for all those who work with UNCI information, and have thus created a new level of clearance in order to deal with this reality.

newcomer is Sensitive Homeland Security Information (SHSI) which includes any information which "relates to the threat of terrorist activity…"[118]

Most recently, the Department of Homeland Security (DHS) issued a directive requiring all DHS employees and contractors to sign a form acknowledging that under threat of criminal penalty they will only share sensitive but unclassified (see SHSI above) information with those having a need to know. Many are concerned that this new set of restrictions will reduce interagency dialogue as well as communications with industry.[119] In fact, this tangled assortment of "un-classifieds" creates an ideal incubator for repetition of similar failures that were highlighted in the 9/11-commission report.[120] The commission found that the 9/11 attacks might have been prevented had intelligence agencies been better at sharing information.[121] While the types of information listed above are not "classified" per se, the new markings are bound to make inter-agency sharing more difficult and thus less likely.

Furthermore, the 9/11 commission overlooked a factor that is just as important as inter-agency communication at the national level. As a result of the information age, our society has become increasingly reliant upon interdependent systems that cannot be effectively defended by any one or even the aggregation of federal agencies. No longer can the CIA and the DoD alone protect our nations borders against invaders. Neither can

---

[118]*DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements*.

[119]Eileen Sullivan, *Searches and Gag Orders: Homeland Security'S Unprecedented Campaign Cloaks Unclassified Info* [Internet] (FederalTimes.com, 2004 [cited April 20 2005]); available from http://federaltimes.com/index.php?S=537895.

[120]National Commission on Terrorist Attacks, *The 9/11 Commission Report* [Internet] (US Government Printing Office, 2004 [cited 20 April 2005]); available from http://www.gpoaccess.gov/911/index.html, 416-19.

[121]Ibid.

the FBI and the Border Patrol stop terrorists from transiting our borders. Even were the DHS given an all-powerful mandate to coordinate all federal agencies into one, it wouldn't be able to prevent the threats posed by the next war. Instead, the battleground of the next war will include portraits of muddied soldiers as well as those of the unlikely warriors who ply their skills on the keyboard of a computer – affecting the markets of their adversaries and perhaps even their soldiers directly. As a result of the inevitable advent of what some have termed, "Unrestricted Warfare" it is naïve to limit interagency cooperation to federal government agencies. It is even shortsighted to restrict information sharing to state and local agencies. In the modern environment, any national security solution that does not embrace the importance of the industrial sector as well as that of the private citizen is destined to result in national failure. In the information age, *every* citizen is linked to the battlefield in some way, and as such has a 'need-to-know'.

…unsuccessfully

There are several problems with the current government solution to protecting sensitive but unclassified information. The first is exhibited in the fact that despite Herculean effort, currently *not all exploitable information has been removed*. Likewise, no matter how hard it tries, government will *never be able to expunge all harmful information* from the Internet. Finally, and most concerning, is that the more successful government is in removing 'sensitive' information, the more likely it is that it will *isolate important information from those who have a genuine need to know*– a threat to a free and open society and an anathema in the information age. In order to be successful in the information age, information must be shared amongst the right people, not ferreted away into cubbyholes.

In the wake of September 11th, it is more difficult to find raw information which could be used to attack the United States. Only three years ago a Georgia Tech website proudly offered anyone that visited a highly detailed interactive map of all the fiber-optic networks in the state.[122] Other sources which offered exploitable information included military websites with detailed information about key personnel, photographs, telephone numbers, base maps, and alarming amounts of detail about deployments. In fact, until recently, access to potentially damaging information was so prevalent, someone planning an attack might be hard-pressed to make a decision on *which* target to attack. Even though most examples of this type of information have been removed, it is still possible to come across a rare exploitable discovery. One example of this was this author's recent Google search for information regarding the U.S. flotilla of weapons and equipment stored in preparation for conflict overseas. While the information was dated, the government website listed the names and descriptions of the ships involved in this mission, their typical military cargo, and their homeports. A quick email to the webmaster resulted in the speedy removal of the offending pages and a short explanation that they had created a whole new web page from scratch and thought that all the old pages had been deleted.

The second problem with the current solution is that it does not acknowledge the role of the *republisher*. The *republisher* is a person or organization which posts electronic copies of government documents on his/her website. *Republishing* U.S. Government documents does not violate copyright law since government documents cannot be copyrighted. *Republishers* can be broadly sorted into three groups, those who

---

[122]http://maps.gis.gatech.edu/telecomweb/

conduct their activities for financial reasons, patriotic reasons, and those who do so mischievously. The last category is rare. An example of a site which operates under financial motivation is www.globalsecurity.org, a website which offers large quantities of current information (as well as numerous advertisements) about U.S. military order of battle, equipment, deployments, and bases. One of the most notable republishers of defense-related information is the Federation of American Scientists (FAS) (www.fas.org), an organization whose board of directors is composed of many individuals who work either directly or indirectly with the national defense establishment. The members of the FAS most likely see themselves as patriots whose postings do more for increasing transparency in government than reducing national security. Were *these* republishers given a forum in which they could limit their audience to Americans only, it is likely that they would do so. Even if government were to criminalize the republication of government documents, the *transportable* nature of most current electronic documents would still allow for the speedy transfer of sensitive but unclassified documents to destinations around the world.

Furthermore, the action of removing information from government websites does nothing if that information remains available on websites unconnected to the government. It is possible to confirm the location of military vessels anchored in harbor from a thousand miles away by using information available to anyone with an Internet connection and a credit card. One need only purchase and download a high-resolution commercial satellite photo by credit card to determine that a military ship is in harbor. Using the live data feed from a shore-based webcam, the agent can confirm the identity and exact location of the ship in question. In time of conflict this information could be

extremely damaging and there is little that can be done to prevent a creative adversary from creatively assembling various sources to create meaningful and exploitable intelligence.

A recent government-sponsored report on the potential threat of government-published geospatial data found that the U.S. government has succeeded in removing all data that is both *useful* to an attacker as well as *unique* in its availability.[123] The report seems to convey a sense of security – that the government is keeping its secrets well. When viewed with a global perspective, however, the report demonstrates that while the government has removed information for which it was the only publisher *(unique)* – much information exists through private sources that can facilitate the same damage. Furthermore, the report failed to adequately assess the extent of how useful information could be once aggregated, conceding that, "new and potentially sensitive information…might be created via the integration of data from diverse sources."[124] At the same time as this report was published, a George Mason University Graduate student did exactly that. Sean Gorman reportedly struck fear into the hearts of the national security establishment when he mapped "every business and industrial sector in the American economy [overlaid with] fiber-optic network that connects them."[125] He had used publicly available geospatial data, which when aggregated visually depicted the most vulnerable points of the United States' telecommunications architecture.

---

[123]John Baker, "Mapping the Risks: Assessing Homeland Security Implications of Publicly Available Geospatial Information," xx.

[124]Ibid.

[125]Laura Blumenfeld, *Dissertation Could Be Security Threat: Student's Maps Illustrate Concerns About Public Information* [Internet] (The Washington Post, 2003 [cited 20 April 2005]); available from http://www.washingtonpost.com/ac2/wp-dyn/A23689-2003Jul7?language=printer.www.washingtonpost.com/

Congress has been aware of a similar security flaw for several years through the testimony of Robert Dacey who has warned that publicly available information such as, "the filings of the Federal Energy Regulatory Commission (FERC), industry publications, maps, and material available on the Internet—[are] sufficient to allow someone to identify the most heavily loaded transmission lines and the most critical substations in the power grid." [126]

Information truly *is* power and how information is handled is of vital interest to the nation. Ironically, information that is kept too secure is of no use – or even damaging, while information shared too liberally can lead to its own damage. This paradox has never been more acute than today. Fortunately, the information age also offers tools to manage information which were previously unimaginable. It is now possible to create databases with user rights and privileges associated with each individual string of data. Each field of information in a given database can reflect different information to different users based on a given user's permission level. Furthermore, the information age affords the opportunity for cryptographic protection of data sent over unsecure channels like the Internet for at least the next 50 years.[127]

These two factors, tailored data and cryptography, now make it possible for an appropriately privileged individual to remotely and securely access limitless amounts of data over the Internet.

While the private sector in the U.S. has moved as quickly as possible to capitalize – in every sense of the word – on the possibilities inherent in personal computing power

---

[126] Robert F. Dacey, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," (U.S. General Accounting Office, 2004), 14.

[127] Schneier, *Secrets and Lies: Digital Security in a Networked World*, 100.

and Internet communications, to date it has failed to put much attention on security. The average – and even advanced – user generally cannot discern the security (or lack thereof) afforded by a given product and therefore most often makes his/her choice based on the functionality of the program. As a result, the market demands functionality at the inevitable expense of security.[128]

The U.S. government has been understandably reluctant to step foot into this arena. After all, the U.S. is home to one of the most successful free-market economies and if a problem exists with the market, the market will right itself. The problem, however, does not stop at the doorways of the marketplace, but instead directly impacts directly on national security.

[128]Ibid., 359-60.

4 – A WAY FORWARD

A National Bureau of Standards

Many have attempted to describe the dawn of the Internet as analogous to the heyday of the old West, where the promise of free land and lack of law enforcement created an atmosphere of excitement and danger.[129] In order to address the problem of lawlessness in cyberspace, some suggest deputizing the equivalent of an international coalition of cyber-judges and sheriffs who will, "instill greater ethical sensitivity," "[create laws to] define bounds of privacy and acceptable behavior," create Computer Network Attack (CNA) prohibition treaties between nations, give system owners a greater sense of responsibility, and create teams of "cyber-intelligence" monitors.[130]

While this solution might at first appear sound, it cannot work. The very structure of the Internet will not allow it because of the difficulty in enforcing law in the multinational arena. Moreover, a portion of the malicious actors likely emanate from the state security services and it is unlikely that governments will find enough common ground to abandon the opportunity to leverage the power of information covertly against their adversaries.

Traditional hierarchical solutions will not work in a decentralized, knowledge-based, networked environment. Just as the NSSC demonstrates a hierarchical approach, so too do many solutions to Internet insecurity. In the hierarchical model a chief authority serves to provide information to, and thus wields power over, the members of

---

[129]Helen McLure, "The Wild, Wild Web: The Mythic American West and the Electronic Frontier," *The Western Historical Quarterly* 31, no. 4 (2000).

[130]Lukasik, Goodman, and Longhurst, *Protecting Critical Infrastructures against Cyber-Attack*, 25-26.

the group and the citizens of the state.[131] The Internet, on the other hand, represents a radical change in the way in which information is passed. Now the individual is empowered by his ability to seek and gain information on his own.

Any successful approach to securing the Internet must include an understanding of the truly revolutionary nature of the Internet. One author has suggested that the United States create a set of rules and regulations for the Internet in much the same manner as the U.S. National Highway System. He further suggests that the network be put under military direction and control since the military has shown itself to best understand information security.[132] The wisdom in this proposal is the understanding that commerce is the fuel which ultimately drives the nation, and that the Interstate Highway system offers a strong parallel to the so-called "information superhighway." The analogy is not perfect, however, in that the Interstate Highway System is not trans-national and the size and types of vehicles (the packets and how they are switched) has already been regulated. Rather than attempt to regulate the traffic, government needs to provide a one-time infusion into the process by establishing a standard for authentication and encryption that can be used by all U.S. citizens.

It is not necessary for government to take any role in the administration of the Internet backbone or any other portion of its architecture. Instead, government should focus efforts in an area which it has heretofore neglected: establishing national standards for information assurance (IA) – beginning with authentication and encryption.

---

[131]Even in the democratic state such as the U.S. certain hierarchies still exist today: the two major political parties, the media (for the most part dominated by several 'media moguls'), churches, corporations, and even unions.

[132]O'Hara, "Department of Homeland Security Policy for Defense of Cyberspace", 9-10.

Much in the same manner as the National Bureau of Standards gave the customer at the deli the assurance that one pound of cheese really was one pound, the consumer must be given the means to be absolutely sure that his transaction with another over the Internet really is the transaction he thinks it is. Furthermore, the deli customer must be confident that his wallet will not be stolen while he makes his purchase or his home ransacked while he is gone. In the same way, the Internet consumer must also be given a reasonable assurance that his transactions are private and not exploitable.

The National Bureau of Standards, now called the National Institute for Standards and Technology (NIST), performs the same function as it did years ago – assuring customer and shopkeeper alike that there is one standard. Interestingly, the NIST is very involved today in establishing standards for networking and computer security for the nation. These standards are not binding, however, and there are no significant incentives for private individuals or even corporations to implement NIST suggestions. Even were the current lists of NIST suggestions for secure computing voluntarily implemented by all U.S. citizens, this would still not solve the problem of compartmentalized sensitive but unclassified information.

Recently, in direct response to Homeland Security Presidential Directive number 12, the NIST published the standard for a common E-identification card for all federal governmental employees.[133] Within the year, all federal governmental employees and contractors are required to possess a card that meets the baseline requirements of NIST standard FIPS-201. The card is based on the "smart-card" standard and includes a visible photograph of the employee along with a computer chip that stores, among other things, a

[133]Bush, *The National Strategy to Secure Cyberspace*.;George W. Bush, *Homeland Security Presidential Directive/Hspd-12* [Internet] (The White House, 2004 [cited 20 April 2005]); available from http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

digital copy of the employee's fingerprint. Prior to being issued the card, the employee must go through an identification process that is currently more stringent than that for the issuance of a U.S. passport. The employee must first be sponsored by an agency, and then present two forms of identification. Once the employee's identification is established, his photo is taken and his fingerprints are digitized and stored on the card to serve as biometric identification. Once issued the PIV (Personal Identity Verification) card, in order to access a given computer system the employee must enter a PIN number to unlock a coded message (encrypted private key). Once verified as the correct message, the system allows the user entry. In order to compromise the card a malicious agent must be both be in possession of the card for some time as well as have access to extremely expensive specialized equipment. Compared to magnetic stripe cards (such as most U.S. credit cards) whose data can be duplicated by a child with a $500 tool available on the Internet, or a easily forged driver's licenses, these cards mark a technological leap forward in both in the physical and Internet realm.

The standardization of the "E-identification" card (or PIV) among federal government employees means that intra-governmental databases may be used with a reasonably high expectation that the user at the other end is actually who she says she is. In the past, systems administrators of government computers have been reliant on passwords alone as security measures. As mentioned earlier, passwords are generally very easy to divine using "social engineering" – or just checking under the keyboard. In the case of the PIV, if the card is ever lost, the user will place a telephone call and have a 'revocation certificate' will be issued preventing the card from ever being used thereafter.

While there are no "silver-bullets" in the security world, the PIV raises the bar for potential adversaries wishing to gain entry into government computer systems.

What's not to like?

The PIV falls short in two areas. First it does not allow for usage outside of the federal workplace. Second, federal workers and contractors are the only individuals being afforded the opportunity to be issued a PIV card. The current plan calls for the card to be used by federal employees and contractors as a means of accessing government computer systems only.[134] This means that while federal employees may be able to use this card in their off time as a means of visual identification, its most powerful feature – an encrypted private key that serves as an extremely strong authentication measure is unusable for private transactions. As such its value becomes something akin to that of a driver's license – a notoriously easy document to forge. For under $100 dollars you can mail order a forged driver's license from the state of your choice from an agency in South Africa.[135] If you have a larger budget and require more confidentiality you can purchase your own ID card printing machine for several thousand dollars.[136] One ID card forger who worked with a terrorist cell testified in 2003 that, "If you have the right connection, you can get anything."[137]

---

[134] *Frequently Asked Questions About the Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors*.

[135] http://www.fakeidguru.com/ is just one of many overseas suppliers of U.S. ID cards.

[136] http://www.idwholesaler.com/

[137] *Fake U.S. Ids Easy for Terrorists* [Internet] (CBS News.com, 2003 [cited 20 April 2005]); available from http://www.cbsnews.com/stories/2003/09/09/attack/main572405.shtml. Of course, if you really want a perfect forgery it is best to steal the equipment straight from the source. See: "200 Blank Id Cards Stolen from Military," *The Washington Times*, 17 May 1998. and more recently an enormous theft of 1,700 blank licenses and printing equipment: Steve Friess, *Identity Theft in Las Vegas Raises Terror Concerns* [Internet] (The Boston Globe, 2005 [cited 20 April 2005]); available from http://www.boston.com/news/nation/articles/2005/03/19/.

Neither will an employee be able to use her card to verify her identity online even though this is exactly the purpose for which the card was designed. Under the current rules, banks and other commercial outlets will be prohibited from verifying the cardholder's identity via the encrypted key. Likewise, the employee will be unable to utilize the encryption capabilities of the card. For purposes of securing and authenticating private communications over the Internet this card has all the security attributes of a 2" x 3" piece of white plastic.

The other problem with the scope of the program is that it is limited to employees and contractors of federal government agencies only. The federal government cannot be successful in the information age without the partnership of its state, local, and private compatriots. If the PIV implementation remains at the federal level the gaps between federal, state, and local law enforcement will never be fully bridged. Instead of a free-flowing sharing of information over permissions-enabled databases, federal sources will be reluctant to share information with others who "don't have the card". Likewise, local sources will be reluctant to pass critical information higher because of the existing divide. Diligent private citizens and corporations who would otherwise be thrilled to play a role in homeland defense also have no envisaged role in the current PIV scheme.[138]

Without widespread deployment and the provision for private use the PIV card can hardly be considered a fix for the nation's Internet security woes. This begs the questions, though, of how a national E-authentication card would be deployed, what advantages it would bring, and finally, what drawbacks are inherent in such a system.

---

[138]Some examples of active citizens who will be further distanced by the current program include volunteer firefighters, Amateur Radio Emergency Service (ARES)/ Radio Amateur Civil Emergency Service (RACES) volunteers, and a host of others.

Privacy Revisited

The most widely used and accepted identification in the United States today is the state driver's license. In order to obtain a driver's license an applicant must report in person to a local bureau of motor vehicles and present a birth certificate, a social security card, a utility bill addressed to the applicant. Each of these documents is relatively easy to forge and there is very little to prevent a determined criminal from obtaining identification under multiple names. Furthermore, disparity exists between both the quality of cards (some are more easily forged than others) as well as quality of the authentication process itself (some states are more stringent than others in their application process). The incorporation of a biometric check, such as the taking of fingerprints, would make it increasingly difficult for an applicant to obtain multiple identities since every new application will be checked against a national registry of existing fingerprints.[139] Lastly, the driver's license is of little use in cyberspace as an identification tool. In order to negate the inherent weakness of the state driver's licensing system as a means of identification (both physical and cyber), the federal government should, through its standards body (NIST), create a national standard for identification that will serve to enhance both individual, corporate, and by extension, national security.

The soon-to-be implemented PIV standard seemingly comes very close to an ideal (for the time-being) identification card. It incorporates the three fundamental elements of authentication *something you know, something you have, and something you are*; the PIN, the card itself, and the user's fingerprint. But under the current implementation plan

---

[139]Even fingerprint biometrics does not0 434 248.27982 Tm(eem)Tj1on plan

it will not work to dramatically enhance national security, nor will it add to national prosperity. Instead, in order to work, the NIST standard must be open for use by all. Every citizen and every institution must be able to access the full functionality of the device. First, the device must be able to serve as a form of physical identification. Industry and government alike should be able to use the full functionality of the encryption enabler (PKI) embedded within the device in order to assist in physical access control. Next, and most importantly, the device standard must allow users to communicate securely with anyone of their choosing. Users must be assured that no one, including government, can eavesdrop on their conversations and electronic transactions.

This last element is crucial. The mere mention of a "national ID" sends shivers up the spines of scores of Americans. For many, a national identification is synonymous with government oppression. All too often, governments have used national identity cards to control information and to oppress dissenters. Two nations in recent history stand out for both their comprehensive identification systems and their brutality towards elements of their citizenry: Nazi Germany and apartheid South Africa.[140] Yet, if the Internet truly heralds a revolution in information flow – and information truly is power – then by failing to ensure the possibility of *information assurance* for the entire citizenry, the United States is in a position to lose power rather than gain it in the information age. The "first link in the security system chain" is the positive identification and authentication of a given user. If this cannot be assured, then any and all other

---

[140]Investigative reporters have written that oppressive regimes such Germany under the Nazi party and South Africa under white rule could not have been nearly as efficient without the support of state-of-the-art computing power provided by suppliers such as the International Business Machine (IBM) Corporation and its subsidiaries. Paul Festa, *Probing IBM's Nazi Connection* [Internet] (CNET News.com, 2001 [cited 19 April 2005]); available from http://news.com.com/2009-1082-269157.html, and Thomas Conrad, "Machines That Help Make Apartheid Run," *The New York Times*, 18 May 1985.

transactions are suspect.[141] In order to bridge the gap between the maintenance of national power and citizen's rights, any identification scheme must enable encryption, anonymity, and be voluntary.

The most crucial element of the free flow of information is the assurance that individual communications will remain private, free of intrusion by the government or anyone else. This is essential in commerce and private communications. If individuals and businesses are not assured that others, including government, cannot read their confidential communications, information flow will slow, stifling the economy. Today, the average user does not encrypt email because it is difficult to do even though most know that every node through which a packet has passed can read their email. An E-identification card with embedded PKI would make encrypted Internet communications the default standard.

Like the ability to encrypt, the ability of a private citizen to conduct a transaction anonymously, should he desire, is essential to ensuring privacy. The Internet as it is currently constructed makes this incredibly difficult. Instead, using "web analytics" businesses and intelligence agencies are able to aggregate immense amounts of information about individuals and groups, "each time [someone] accesses the Internet, they leak pieces of information to watchful competitors, hackers and online predators."[142] While the government need not be involved in many aspects of ensuring user anonymity, the E-identification standard must incorporate a national standard for user anonymity. One example of how such a standard might work has been described in detail by a cryptologist by the name of Dr. David Chaum. While the details are too complex to

---

[141]Bush, *The National Strategy to Secure Cyberspace*, 46.

[142]*Protecting Corporations from Internet Counter-Intelligence*, 2.

describe in this paper, but Dr. Chaum's work builds on the fundamentals of PKI as described in chapter 3. The system enables people to spend money, and even vote anonymously yet securely.[143]

Finally, while no one should be forced to obtain an E-authentication card, this card will likely become the identification of choice because of its stringent authentication requirements. Just as it is extremely difficult to cash a check without a driver's license (another optional form of identification), so too would the E-authentication card be adopted by all sorts of entities seeking positive identification, both off and on-line. One factor that mitigates the social risks of a de facto national ID card is a privatized distribution system. Just as some private companies have been certified to authenticate and distribute the PIV, so too should a national E-identification card be privatized. The role of the federal government in the E-identification schemes should be limited to creation and enforcement of a standard. In this way, the PKI remains in private hands rather than government, adding a "trusted third party" as a buffer between the citizen and government.

National Security Revisited

The advantages of a national E-identification standard for government are chiefly that databases may now be created that can be accessed from anywhere by anyone with the appropriate privileges. Instead of relying on the easily exploitable user ID and password scheme, government can be reasonably assured that the user on the other end is who he says he is – and deliver the appropriate information to him, whether he be state, federal, local, volunteer, or based on location, a citizen with a need to know. Since 2001

---

[143]Chaum's system is able to provide for the principle of non-repudiation while enabling anonymity. See, David Chaum, "Achieving Electronic Privacy," *Scientific American* (1992).

much information has been removed from the Internet that was of important interest to concerned citizens. While this removal continues to be important for national security, there is no excuse for not creating a system that would allow authorized citizens to access sensitive information relating to their local area. One example of such information includes information published by the government under the federal "Right-to-Know Act" aimed at empowering citizens living near toxic chemical release sites to be better aware of potential environmental and health risks. The same information in the wrong hands could be used by terrorists to create an ecological disaster, and for this reason it has been removed.[144] Other examples include information pertaining to offshore facilities that might be vulnerable to attack such as oil rigs. In this case, too, citizens who transit the waterways in the vicinity of the facility need to know particular details in order to safely transit the area.[145] Certainly thousands of such examples exist and an E-identification card would allow government to deliver the right information to the right people – both private citizens as well as public servants, securely.

---

[144]John Baker, "Mapping the Risks: Assessing Homeland Security Implications of Publicly Available Geospatial Information," 76.

[145]Ibid., 85.

CONCLUSION

The information age has wrought both triumph and challenge. Today we can order anything from anywhere in the world and expect its arrival within days. Because of information technology we are able process vast amounts of information in order to make better decisions more quickly than ever before. There is a dark side, however. Just as the world has gotten smaller for us, so too has it become easier for our enemies to discover and exploit our vulnerabilities. On September 11, 2001 one such enemy did just that, using information available on the Internet to help plan for the attack.

In response the U.S. government has taken prudent measures to reduce the amount of potentially sensitive information on the Internet. This has had the unfortunate side effect of compartmentalizing information from those for whom it was originally posted, the American people.

Another related issue is the epidemic infection of private computers with various forms of malware, many of which are designed to conduct a form of espionage on personal computers. This is a threat to U.S. national security in that it demonstrates the ability of malicious actors to directly affect the integrity of our national network, and it rightly has the effect of reducing citizen confidence in the integrity of their Internet transactions.

In order to restore the integrity of Internet transactions and allow for information sharing between citizens, corporations, local and state governments, the U.S. government must act decisively to implement a nation-wide Internet identification card. In order to be successful the device must meet following criteria: it must be able to authenticate the user with a high degree of certainty; it must enable encrypted communications and the

ability to provide digital signatures; it must allow for the option of anonymous transactions should the user desire (e.g. voting, financial dealings, transit, etc…); it must be available to all citizens; it must be optional.

Once implemented, the federal government can republish once stricken information on a secure Intranet database where citizens can logon to view information tailored to them and their need-to-know based on location and position. This capability will allow government to reconnect – digitally – with its citizens as well as provide for a standardized method of communication between state, local, and volunteer first responders. Furthermore, the card, once issued would enable citizens to conduct private banking and other transactions with the reasonable assurance that such transactions are secure from malicious actors.

The benefit for individual citizens is threefold. First, this solution opens a new avenue for dialogue with the federal government. Second, this proposal, once adopted, would effectively halt all current methods of identity theft. Third, the renewed trust wrought by the increase in secured communications would renew consumer confidence in the Internet, likely resulting in increases in consumer spending.

We will only be able to ensure the continuation of the "blessings of liberty" for our children if we are able to take creatively exploit the opportunities presented to us by the information revolution.[146]

Proposal for further study

The E-authentication card does not solve the underlying problem of an unsecure kernel. Because the numerous flaws in the kernel of one of the most popular operating

---

[146] *The Constitution of the United States*.

systems, even the most diligent computer user cannot be entirely assured of the security of her system. As a result, even a strong authentication piece such as a PIV card can still be exploited by a "man-in-the-middle" attack.[147] For communications requiring a particularly high level of security such as government, banks, and industry, the following solution is worth examining. Instead of establishing an Internet connection over a potentially compromised or compromisable operating system, organizations requiring a higher level of security could publish their own bare-bones, secure kernel OS and browser on removable media (such as a CD), and E-identification card reader. The kernels of the OS and browser would be small, secure, and simple; their sole purpose being the establishment of a secure connection with a particular host and to display its data. Once inserted, the local machine would boot from that media and then make an E-identification card enabled connection to the host. Once securely online the browser acts as a terminal emulator and the user would be able to type as though he were on his own machine.[148]

In this manner, those transactions that require the highest levels of security such as banks, corporations, and government could ensure the integrity and security of information flow in a way that is not possible today. Though slightly cumbersome, it is imaginable that an individual might keep one or two such CDs (e.g., one for work and another one for banking.)

---

[147]Schneier, *Secrets and Lies: Digital Security in a Networked World*, 222-24.

[148]It is worth noting the several ways in which security could still be breached using this method: shoulder-surfing (remote camera or in situ), keystroke logging (inline only). All of these methods require physical intrusion, however, upping the ante considerably – increased risk of getting caught.

APPENDIX 1 – GLOSSARY

- **Archive –** a bundle of other files contained in one file itself.[149]
- **Best Practices** – Generally accepted system security principles in current use.[150]
- **Cache –** a pool of entries.[151]
- **Classified Information –** Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.[152]
- **Computer Network Attack (CNA) –** Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.[153]
- **Computer Network Defense (CND) –** Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.[154]
- **Computer Network Exploitation (CNE) –** Intelligence collection and enabling operations to gather data from target adversary automated information systems (AIS) or networks.[155] Or;
- **Computer network exploitation (CNE) –** Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. CNE is composed of two types of activities: (1) enabling activities designed to obtain or facilitate access to the target computer system where the purpose includes foreign intelligence collection; and, (2) collection activities designed to acquire foreign intelligence information from the target computer system.[156]
- **Computer network operations (CNO)** – Comprises CNA, CND and CNE collectively.[157]

---

[149] *Wikipedia*.

[150] Marianne Swanson and Barbara Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Internet] (NIST, 1997 [cited 28 April 2005]); available from http://csrc.nist.gov/publications/nistpubs/, 1.

[151] *Wikipedia*.

[152] *JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

[153] Ibid.

[154] Ibid.

[155] *DoD Directive 3600.1, Rev. 1: Information Operations (IO)*.

[156] Ibid.

[157] Ibid.

- **Cookie –** a packet of information sent by a server to a World Wide Web browser and then sent back by the browser each time it accesses that server.[158]
- **Critical Infrastructure Protection —** Department of Defense (DOD) program to identify and protect assets critical to the Defense Transportation System. Loss of a critical asset would result in failure to support the mission of a combatant commander. Assets include worldwide DOD, commercial, and civil physical and command, control, communications, computers, and intelligence infrastructures.[159]
- **Cyberspace** – The online world of computer networks.[160]
- **Deep Web –** name given to the publicly accessible pages on the World Wide Web that are not indexed by search engines. It consists mainly of dynamically generated pages that are based on responses to database queries.[161] (Also referred to as: Hidden Web, Invisible Web)
- **Defensive Information Operations –** The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.[162]
- **Dumpster-Diving –** used for searches through discarded material looking for otherwise unavailable information. Businesses and individuals frequently discard information including printouts with passwords, credit card numbers, business planning and so on; some of this can be recovered by determined divers.[163]
- **Extranet** – two or more intranets with network connectivity.[164]
- **Information –** Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.[165]
- **Information Assurance (IA) –** Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and

---

[158]*Wikipedia*.

[159]*JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

[160]*Merriam-Webster Dictionary* [Internet] (Merriam-Webster, 2005 [cited 26 April 2005]); available from www.m-w.com.

[161]*Wikipedia*.

[162]*JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

[163]*Wikipedia*.

[164]Ibid.

[165]*JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

reaction capabilities.[166]

- **Information Operations (IO) –** Actions taken to affect adversary information and information systems while defending one's own information and information systems.[167]
- **Intelligence —** 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
- **Internet –** the publicly available worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols.[168]
- **Intranet –** a local area network (LAN) used internally in an organization to facilitate communication and access to information that is sometimes access restricted.[169]
- **ISP-blocking** – the act of preventing access to a website from certain IP addresses.[170]
- **ISP-spoofing** – the act of tailoring web page delivery to originating IP addresses[171]
- **Logical Access Control** – The ability to do something with a computer resource (e.g. use, change, or view). Best practices dictate that "users should be granted access only to the resources which they need to perform their official functions."[172]
- **National Information Infrastructure (NII)** – The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The [NII] encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmissions lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component.[173]
- **Open Source Intelligence –** Information of potential intelligence value that is available to the general public.
- **Operational Security (OPSEC) –** A process of identifying critical information

---

[166]Ibid.

[167]Ibid.

[168]*Wikipedia*.

[169]Ibid.

[170]*Protecting Corporations from Internet Counter-Intelligence*.

[171]Ibid.

[172]Swanson and Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 46.

[173]*JP 1-02: Department of Defense Dictionary of Military and Associated Terms*.

and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.[174]

- **Pharming** – the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic to that web site to another web site.
- **Phishing** – the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by masquerading in an official-looking email, IM, etc. as someone trustworthy with a real need for such information.[175]
- **Public Key Infrastructure (PKI) –** an arrangement which provides for third-party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.[176]
- **Robot –** a program which browses the World Wide Web in a methodical, automated manner.[177] (See also Spider)
- **Shoulder-Surfing –** shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter their PIN at an automated teller machine, use a calling card at a public pay phone, or enter passwords at a cybercafe or airport kiosk.[178]
- **Social Engineering –** the practice of obtaining confidential information by manipulation of legitimate users.[179]
- **Spider** – a program which browses the World Wide Web in a methodical, automated manner.[180] (see also Robot)
- **Supervisory Control and Data Acquisition system (SCADA)** – are used in industrial and civil engineering applications to control distributed systems from a master location. SCADA is a very broad umbrella that describes solutions across a large variety of industries, including but not limited to the following: Electric power generation, transmission and distribution, Environmental control systems,

---

[174]Ibid.

[175]*Wikipedia*.

[176]Ibid.

[177]Ibid.

[178]Ibid.

[179]Ibid.

[180]Ibid.

Traffic signals, Water management systems, Mass transit systems, and Manufacturing systems.[181]

- **Terabyte –** a unit of information or computer storage equal to one trillion (one long scale billion) bytes.[182]
- **Terminal Emulator –** a program that emulates a "dumb" video terminal within some other display architecture. A terminal emulator inside a graphical user interface is often called a terminal window.[183]
- **Trojan** – a malicious program that is disguised as legitimate software.[184]
- **Uniform Resource Locator (URL)** – a standardized address for some resource (such as a document or image) on the Internet.[185]
- **Virus** – virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.[186]
- **Web –** an information space in which the items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers (URI).[187]
- **Web Analytics** – Web analytics is the assessment of a variety of data, including Web traffic, Web-based transactions, Web server performance, usability studies, user submitted information and related sources to help create a generalized understanding of the visitor experience online.[188]
- **Web Host –** a service that provides Internet users with online systems for storing information, images, video, or any content accessible via the web. Web hosts are companies that provide space on a server they own for use by their clients as well as providing Internet connectivity, typically in a data center.[189]
- **Worm** – a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.[190]

---

[181] *Protecting Corporations from Internet Counter-Intelligence*.

[182] *Wikipedia*.

[183] Ibid.

[184] Ibid.

[185] Ibid.

[186] Ibid.

[187] Ibid.

[188] Ibid.

[189] Ibid.

[190] Ibid.

BIBLIOGRAPHY

21 Steps to Improve Cyber Security of SCADA Networks. 2002! In, Department of Energy, President's Critical Infrastructure Protection Board, http://oea.dis.anl.gov/documents/21StepsBooklet.pdf. (accessed 2004).

"200 Blank Id Cards Stolen from Military." *The Washington Times*, 17 May 1998, 15.

"Access to Government Information Post September 11th." *OMB Watch*, Feb 1 2002!

AOL/NCSA. "AOL/NCSA Online Safety Study." America Online & National Cyber Security Alliance, 2004.

Arkin, William. *Code Names: Deciphering U.S. Military Plans, Programs and Operations in the 9/11 World*. Hanover, NH: Steerforth Press, 2005.

Ashley, Bradley K. 2003. Anatomy of Cyberterrorism: Is America Vulnerable? In, Air War College, www.au.af.mil/au/awc/awcgate/awc/ashley.pdf. (accessed 30 October, 2004).

Bashki, Prashant. "Open Source Intelligence: A 'Force Multiplier'." In *NATO Open Source Intelligence Reader*, 95-97: NATO, 2002.

Blumenfeld, Laura. 2003. Dissertation Could Be Security Threat: Student's Maps Illustrate Concerns About Public Information. In, The Washington Post, http://www.washingtonpost.com/ac2/wp-dyn/A23689-2003Jul7?language=printer. (accessed 20 April, 2005).

Buchalter, Alice R., John Gibbs, and Marieke Lewis. 2004. Laws and Regulations Governing the Protection of Sensitive but Unclassified Information. In, Federal Research Division, Library of Congress, http://www.fas.org/sgp/library/sbu.pdf. (accessed 27 April, 2005).

Bush, George W. 2004. Homeland Security Presidential Directive/Hspd-12. In, The White House, http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html. (accessed 20 April, 2005).

———. 2003. The National Strategy to Secure Cyberspace. In, http://www.whitehouse.gov/pcipb/. (accessed 2004).

Chaum, David. "Achieving Electronic Privacy." *Scientific American* (1992): 96.

Conrad, Thomas. "Machines That Help Make Apartheid Run." *The New York Times*, 18 May 1985, 24.

The Constitution of the United States. 1789. In, Heritage.org, http://www.heritage.org/. (accessed 14 Feb, 2004).

Cracking Enigma. n.d. In, ThinkQuest, http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/bombe.shtml. (accessed 19 April, 2005).

Creating a Trusted Network for Homeland Security. 2003. In, Markel Foundation, http://www.markle.org/. (accessed 20 April, 2005).

Dacey, Robert F. "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems." U.S. General Accounting Office, 2004!

———. "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems." U.S. General Accounting Office, 2004.

A Decade of Adoption: How the Internet Has Woven Itself into American Life. 2005. In, www.pewinternet.org, http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf. (accessed 20 April, 2005).

DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements. 1999. In, v 1.2, Defense Informations Systems Agency, www.fas.org/sgp/othergov/dod/genser.pdf. (accessed April 20, 2005).

DoD Directive 3600.1, Rev. 1: Information Operations (IO). 2001. In, Department of Defense, http://www.iwar.org.uk/iwar/resources/doctrine/DOD36001.pdf. (accessed 28 April, 2005).

Fake U.S. Ids Easy for Terrorists. 2003. In, CBS News.com, http://www.cbsnews.com/stories/2003/09/09/attack/main572405.shtml. (accessed 20 April, 2005).

Festa, Paul. 2001. Probing IBM's Nazi Connection. In, CNET News.com, http://news.com.com/2009-1082-269157.html. (accessed 19 April, 2005).

FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures. Washington, D.C.: Headquarters, Department of the Army, 2003.

FOIA Reference Guide. 2005. In, Department of Justice, http://www.usdoj.gov/04foia/04_3.html. (accessed 27 April, 2005).

Frequently Asked Questions About the Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors. 2005. In, National Institute of Standards and Technology, http://www.nist.gov/public_affairs/releases/piv_faqs.htm. (accessed 27 March, 2005).

Friess, Steve. 2005. Identity Theft in Las Vegas Raises Terror Concerns. In, The Boston Globe, http://www.boston.com/news/nation/articles/2005/03/19/. (accessed 20 April, 2005).

Gagnon, Benoît. 2004. Are We Headed for a "Cyber-9/11?": The Failure of American Cyberstrategy. In, Raoul-Dandurand Chair Website, http://www.dandurand.uqam.ca/download/pdf/isa2004/gagnonb.pdf. (accessed 21 April, 2005).

Gilder, Tom. ! IE Clipboard Stealing Vulnerability. In, http://tom.me.uk/clipboard/. (accessed 25 April, 2005).

Graham, Robert. 2001. Carnivore Faq. In, http://www.robertgraham.com/pubs/carnivore-faq.html. (accessed 30 October, 2004).

How Much Information? 2003. In, University of California, Berkeley, http://www.sims.berkeley.edu/research/projects/how-much-info-2003/. (accessed 20 April, 2005).

Identity Theft Resource Center. 2005. Facts and Statistics. In, Identity Theft Resource Center, http://www.idtheftcenter.org/facts.shtml. (accessed 20 April, 2005).

Information Vulnerability and the World Wide Web. 1998. In, Department of Defense, http://www.defenselink.mil/other_info/depsecweb.pdf. (accessed 5 Feb, 2005).

Jenkins, James M. "Computer Network Defense: DoD and the National Response." Air War College, 2002.

John Baker, Beth E. Lachman, David R. Frelinger, Kevin M. O'Connell, Alexander C. Hou, Michael S. Tseng, David Orlosky, Charles Yost. "Mapping the Risks: Assessing Homeland Security Implications of Publicly Available Geospatial Information." Pittsburgh, PA: RAND Corporation, 2004.

JP 1-02: Department of Defense Dictionary of Military and Associated Terms. 2001. In, Department of Defense, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. (accessed 25 March, 2005).

Kevin D. Mitnick, William L. Simon, Steve Wozniak. *The Art of Deception: Controlling the Human Element of Security*: Wiley, 2002.

Liang, Qiao, and Wang Xiangsui. *Unrestriced Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

Lukasik, Stephen J., Seymour E. Goodman, and David W. Longhurst. *Protecting Critical Infrastructures against Cyber-Attack*. Translated by 359: 1. New York: Oxford University Press, 2003.

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. "Impact of Artificial "Gummy" Fingers on Fingerprint Systems." Paper presented at the SPIE, Optical Security and Counterfeit Deterrence Techniques IV, 24-25 January 2002.

McLure, Helen. "The Wild, Wild Web: The Mythic American West and the Electronic Frontier." *The Western Historical Quarterly* 31, no. 4 (2000): 457-76.

Merriam-Webster Dictionary. 2005. In, Merriam-Webster, www.m-w.com. (accessed 26 April, 2005).

National Commission on Terrorist Attacks. 2004. The 9/11 Commission Report. In, US Government Printing Office, http://www.gpoaccess.gov/911/index.html. (accessed 20 April, 2005).

O'Hara, Timothy. "Department of Homeland Security Policy for Defense of Cyberspace." U.S. Army War College, 2003.

Opfer, Steven E. 1999. The History of the Internet According to Itself: A Synthesis of Online Internet Histories Available at the Turn of the Century. In, http://members.cox.net/opfer/Internet.htm. (accessed 19 April, 2005).

The Privacy Act of 1974: 5 U.S.C. § 552a. 1974. In, http://www.usdoj.gov/04foia/privstat.htm. (accessed 27 April, 2005).

Protecting Corporations from Internet Counter-Intelligence. n.d. In, Anonymizer, http://www.anonymizer.com/enterprise/info/papers.shtml. (accessed 16 April, 2005).

Rathmell, Andrew. 2001. Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations. In, RAND Europe, http://www.nato.int/acad/fellow/99-01/rathmell.pdf. (accessed 20 April, 2005).

Rice, Condoleezza. 2005. U.S. Security Policy: Protecting the Nation's Critical Infrastructure. In, U.S. Department of State, http://usinfo.state.gov/journals/itps/0301/ijpe/pj61rice.htm. (accessed 20 April, 2005).

Roberts, Paul. 2005. Microsoft Warns of New Security Threat: System Monitoring Programs, Called Rootkits, May Pose a Serious Danger to Your Pc. In, PC World, http://www.pcworld.com/resource/article/0,aid,119720,pg,1,RSS,RSS,00.asp. (accessed 25 April, 2005).

Said, Carolyn. 2004. Revolutionary Chapter Google's Ambitious Book-Scanning Plan Seen as Key Shift in Paper-Based Culture. In *San Francisco Chronicle*, http://www.sfgate.com/cgi-bin/. (accessed 20 April, 2005).

Schneier, Bruce. 2005. Digital Information Rights Need Tech-Savvy Courts. In, eWeek, http://www.eweek.com. (accessed 29 April, 2005).

———. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley, 2000.

Steinauer, Dennis D, Shirley M. Radack, and Stuart W. Katzke. 1997. U.S. Government Activities to Protect the Information Infrastructure. In, U.S. National Institute of Standards and Technology, http://csrc.nist.gov/publications/secpubs/. (accessed 20 April, 2005).

Sullivan, Eileen. 2004. Searches and Gag Orders: Homeland Security'S Unprecedented Campaign Cloaks Unclassified Info. In, FederalTimes.com, http://federaltimes.com/index.php?S=537895. (accessed April 20, 2005).

Swanson, Marianne, and Barbara Guttman. 1997. Generally Accepted Principles and Practices for Securing Information Technology Systems. In, NIST, http://csrc.nist.gov/publications/nistpubs/. (accessed 28 April, 2005).

Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of "Cyberplanning"." *Parameters*, no. Spring (2003): 112-23.

———. "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice." Fort Leavenworth, KS: Foreign Military Studies Office, n.d.

Toffler, Alvin, and Heidi Toffler. *Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*. New York: Bantam Books, 1990.

USA Technology: Identity Theft'S New Face. 2005. In, ebusinessforum.com. (accessed 20 April, 2005).

Weimann, Gabriel. 2004. www,terror.net: How Modern Terrorism Uses the Internet. In, United States Institute of Peace, http://www.usip.org/pubs/specialreports/sr116.pdf. (accessed 30 Oct, 2004).

What Is Public-Key Cryptography? n.d. In, RSA Laboratories, http://www.rsasecurity.com/rsalabs/node.asp?id=2165. (accessed 29 March, 2005).

Wikipedia. 2005. In, Wikipedia, http://en.wikipedia.org/wiki/. (accessed 25 April, 2005).

Wolf, Gary. 2003. The Great Library of Amazonia. In *Wired Magazine*, http://www.wired.com/news/business/0,1367,60948,00.html. (accessed 20 April, 2005).

Wright, Tom. 1994. Privacy and Electronic Identification in the Information Age. In, Information & Privacy Commissioner - Ontario, http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11395&N_ID=1&PT_ID=11351&U_ID=0. (accessed 20 April, 2005).