

---

## ACKNOWLEDGING THE REVOLUTION: THE URGENT NEED FOR CYBER COUNTERINTELLIGENCE

---

*Geoffrey S. French and Jin Kim*

Computers and Information Technology (IT) have fundamentally changed how people and organizations create, share, and store information, causing the U.S. military to re-think mission execution and resulting in such concepts as the “Revolution in Military Affairs,” “Network-Centric Warfare,” or simply “Transformation.” If intelligence is defined as “secret, state activity to understand or influence foreign entities,”<sup>1</sup> then one could argue that computer networks have caused as large a change in intelligence as they have in military affairs. After all, understanding and influencing an entity requires accessing, exploiting, or manipulating information.

More importantly, by changing the business practices of the U.S. Government, military, and private sectors, computer networks have changed how U.S. adversaries conduct business against the United States. Yet, no discussion of U.S. Counterintelligence (CI) activities has been undertaken with a parallel announcement of a revolution or transformation. Even the attention paid to Information Warfare (IW) or Information Operations tends to approach defensive concepts conservatively, focusing on Information Assurance (IA) and simple security.<sup>2</sup> Little professional or academic discussion of the need for a fundamentally different approach to cyber CI has occurred. Indeed, even the “National Counterintelligence Strategy of the United States of America” treats cyber issues as a long-term goal, calling for the Intelligence Community (IC) to “expand [its] efforts into cyberspace.”<sup>3</sup> This unannounced transformation has been undertaken by Foreign

Intelligence Services (FISs), and the exploitation of U.S. networks is clearly underway. The U.S. CI Community, therefore, needs to accelerate its efforts.

This article begins by defining the mission of cyber CI and provides some concepts on how the CI Community can implement such a mission as well as protect public and private information. The final sections suggest gaps in the current U.S. strategy and describe potential cyber threats.

## DEFINING CYBER CI

U.S. cyber CI has existed *de facto* since the introduction of IT to intelligence, defense, and national security and has grown as FISs have embraced cyber tradecraft. The remote exploitation of computer systems, in particular, allows a low-cost mechanism for anonymous—if not surreptitious—access to information that minimizes the need to recruit assets.

In the late 1990s and the early 2000s, cyber CI first began identifying areas of common interests among the various government agencies' CI programs. In this way, the CI Community started to define a subset of CI that deals specifically with the added capabilities and vulnerabilities of computers and computer networks. As defined by DoD, cyber CI activities are those that identify, penetrate, or neutralize foreign operations, which use cyber as the primary tradecraft methodology as well as FIS collection using traditional methods to gauge U.S. cyber capabilities and intentions.<sup>4</sup> In other words, cyber CI deals with FIS collection where computers and computer networks are either the primary tool or target.

Since the 2001 terrorist attacks, the focus of the National Security Community has shifted primarily to terrorism, with the cyber

threat receiving relatively less attention. For this reason, most of the discussion of cyber CI issues has taken place in areas of government that deal with defensive IW.<sup>5</sup> While the two terms are not interchangeable, both do deal with protecting information and information systems or manipulating information for a defensive advantage. Strategies that *actively* counter FIS collection of sensitive or classified information are relegated to only supporting wartime efforts or clear cases of foreign espionage. The greatest part of the U.S. effort to protect government information is limited to information security or assurance,<sup>6</sup> which gives the U.S. CI Community a reactive role in protecting government systems and largely an ineffective one regarding private information and cyber systems.

#### THE SECURITY ENVIRONMENT FOR GOVERNMENT SYSTEMS

In theory, the role of CI in the information security framework could be minor; the government should be able to secure its own computer networks. The government controls the purchase of hardware and software, sets policy, mandates training, manages patches and security upgrades, and reviews implementation. Any number of government reports, however, reveal that IA is very difficult, frequently resulting in ineffective security.<sup>7</sup> In practice, the vulnerability to cyber exploitation has only grown over recent years. IT networks store more information, transfer it more rapidly, and do so for larger numbers of users and interfaces among networks. Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of users within the system. Nowhere is this more evident than for an outside adversary attempting to penetrate a network. A large number of users means more opportunities to find poor security practices while more connectivity means more potentially vulnerable points of entry. Similarly, the more a network is used, the more potentially useful information it will contain for the FISs.

The problem, however, is larger than attempting to fix the security of an individual system or of a large number of systems. Relying on information security to protect sensitive or classified material from foreign acquisition ignores the fact that people often move sensitive information outside of systems that have the proper protection, as many high-profile cases have shown.

- Former Director of Central Intelligence John M. Deutch, while at home, transferred classified material to his government-owned computer, which was designated “Unclassified Use Only.” To make matters worse, this computer was connected to the Internet.<sup>8</sup>
- In the Kosovo air campaign in 1999, the lack of interoperable secure communications systems among the NATO partners resulted in the frequent use of non-secure communications that reduced operational security and likely led to Serbian interception of U.S. communications during the conflict.<sup>9</sup>
- Wen Ho Lee, a computer scientist at Los Alamos National Labs pleaded guilty to transferring national defense information onto an unsecure computer and making a copy onto a computer tape.<sup>10</sup> The division that Lee worked for had access to specific technical information on U.S. nuclear weapons.<sup>11</sup>
- In 2007, the House Committee on Oversight and Government Reform began an investigation into whether members of the staff of the President of the United States used e-mail accounts other than the official government addresses to share information about sensitive policy matters. Regardless of the legality, the alleged communication reveals that some communication of high-level government policy occurs outside of the control of government systems.<sup>12</sup>

The confluence of both the difficulty of adhering to a strict information security policy and the willingness of users to move data outside of protected networks has radically changed the security

environment. Focusing on protecting classified networks and investigating only the largest-scale computer intrusions is analogous to the Austrians awaiting Napoleon's siege of their fortified positions or the Allied decision in 1940 to hunker down behind the Maginot Line. Just as the French circumvented the fortifications and the Axis forces simply bypassed the most formidable defenses, FISs are likely to focus on the valuable information that exists in unprotected or non-secure networks.

The CI Community has not actively engaged in altering the information security framework even while the numbers of sensitive systems placed on non-secure networks increase. One clear example is military logistics. As commercial-off-the-shelf (COTS) technology has improved, it has played a larger role in U.S. Government and military systems.<sup>13</sup> Web-enabled services and radio frequency identification (RFID) are examples of the modernization of U.S. military logistics, principally in the Battle Command Sustainment Support System (BCS3); RFID and vehicle-tracking systems allow real-time in-transit visibility in the BCS3.<sup>14</sup> Although precautions are in place to limit information on blue forces<sup>15</sup> through access controls and multi-layer security, detailed logistics information can be key to FISs. Networks with COTS software are likely to have vulnerabilities that can result in the loss of confidentiality of the network; as an example, in 1998, teenaged hackers, in an incident referred to as "Solar Sunrise," successfully penetrated these very types of systems—"unclassified logistics, administration, and accounting systems that control [the] ability to manage and deploy military forces."<sup>16</sup> FISs that are attempting to gauge U.S. current combat power, therefore, are more likely to target information on a non-secured system than to take on the more complex task of obtaining classified information on secured systems.

Too frequently the contribution of cyber CI to an organization is completely reactive, limited to incident management, investigations, and damage assessments. A more mature cyber CI effort can be more active, translating an understanding of FIS collection into information

useful to an organization's information security efforts. Insight into adversary tactics, techniques, and procedures in computer network exploitation, for example, can make a cyber CI analyst a valuable advisor to every part of the IA framework, influencing the current defensive posture, near-term acquisition, and long-term enterprise architecture planning. As an irreducible minimum, cyber CI analysis must contribute to the risk assessment performed in the planning stage of new mission-critical IT systems and networks.

## THE SECURITY ENVIRONMENT FOR INFRASTRUCTURE SYSTEMS

Foreign cyber activity for the purpose of obtaining sensitive U.S. information is evident in private industry.<sup>17</sup> The Internet has lowered the risk of FIS espionage, because it provides “an easy, inexpensive, and anonymous way to spot, assess, and target U.S. firms and individuals,” including those who may be willing to ignore or short-circuit export restrictions on sensitive U.S. technologies.<sup>18</sup> Gordon Gekko, the antagonist from the movie *Wall Street*, argued that information is a commodity; modern technology—as well as overseas outsourcing of supply chains and IT-related services—has made it easier for foreign agents to gain discrete access to this commodity. A study sponsored by the FBI found that “nearly nine out of 10 U.S. businesses suffered from a computer virus, spyware, or other online attack in 2004 or 2005 despite widespread use of security software.”<sup>19</sup> The *Economic Espionage Act of 1996* offers little protection, because however severe its sanctions are against offending countries, security remains the responsibility of the individual company. With little fear of prosecution, foreign agents or companies can obtain sensitive information by direct request. Indeed, elicitation is frequently the most common method used by foreign agents to acquire U.S. information and technological data.<sup>20</sup> Attempts to conduct espionage in the United States, especially through cyberspace, will continue due to the demand for

sensitive U.S. information, the relatively low risk of detection, and the abundant supply of vulnerabilities to exploit.

Cyber attacks go beyond espionage. In addition to obtaining information, cyber attacks can exploit a computer network by manipulating the data or sabotaging the system. For example, in 2002, an employee of a U.S. investment and brokerage service—hoping to profit from a drastic reduction in the value of the company's stock—constructed a logic bomb that he encapsulated within computer updates sent from the company's mainframe to approximately 1,000 branch office servers. The malicious code destroyed files on infected hard drives and temporarily shut down the company's communications system. In this case, back up systems allowed the company to continue its trading operations, which prevented a disruption of service.<sup>21</sup> Manipulation or sabotage of a general IT system can lead to severe economic consequences for a company. (In the infamous 1996 case of the logic bomb in the Omega Engineering Corporation system, the interruption in manufacturing cost the company at least \$10 million.<sup>22</sup>) For industrial control systems (ICSs)—a generic term that includes Distributed Control Systems (DCS), Process Control Systems (PCS), and Supervisory Control and Data Acquisition (SCADA) systems—the consequences can also affect people's lives.

The security environment for ICSs is also different from that of IT systems. On one hand, obscurity and isolation can offer some protection. The protocols tend to differ from that of IT operating systems networks, and these systems were not designed to be connected to the Internet or modern protocols. On the other hand, trends are headed in the opposite direction; there is increasing integration with modern protocols and greater degrees of connectivity with business networks or the Internet itself. These trends are worrisome, because ICSs have higher levels of vulnerability to cyber attack for two reasons. First, enforcing strict access control is difficult due to the overriding priority of ensuring the availability of the system. Although the processes involved with infrastructure or manufacturing are automated, they all

require human oversight. In situations that involve changes to the system (such as an overpressure in a pipe or a valve requiring override), the engineer must have instant access and authority to make the necessary adjustments. For this reason, ICSs tend to commit several “cardinal sins” of IT security. Generic log-ins are ubiquitous. Administering specific levels of access or user privileges can be complex—if not impossible—due to incompatibility of hardware or software. Second, patch management is much more difficult for an ICS where it is common to encounter old hardware and software that utilize obscure protocols. Software patches have been known to have unanticipated effects on seemingly unrelated components and processes within an IT network, an unacceptable outcome in an ICS environment. Engineers, therefore, seldom (if ever) apply a patch without explicit consent from the manufacturer of the ICS components. The requisite research and testing can take months, during which time malicious code could emerge, and the system could be exploited.<sup>23</sup>

From an ICS engineering perspective, security is a distant third in the list of IA priorities, that is, if it is considered at all. In some cases, security is simply not part of the system’s design. In others, security was ill-suited (e.g., in slow processors with highly time-sensitive processes, authentication may be impossible).<sup>24</sup> The result is a highly complex information security environment: a system that has limited or no ability to run anti-virus software, authenticate commands, or encrypt its communications. In addition, ICSs use a wider variety of media (from microwaves to modems) and protocols than IT networks. Furthermore, an organization may not control all communications in and out of the system. ICS manufacturers often provide remote maintenance and may even have their own modems or telephone lines. Even complete inventories and war-dialing<sup>25</sup> may not expose all of the entry points into an ICS. For these reasons, the vulnerability of ICSs to a cyber attack is higher than that of business networks, and the consequences can be worse.<sup>26</sup> In this area—with such severe vulnerabilities—CI must work to supplement security where the information security framework cannot. The current threat, however,

is low. Only a few nations, organizations, or other entities have both the capability and intent to attack ICSs. The CI Community, however, cannot expect this threat to remain static indefinitely.

### GAPS IN THE CURRENT STRATEGY

The need to maintain traditional CI methods and approaches is evident in today's national security environment. Especially in counterterrorism efforts, the need for recruiting assets for information or action is critical to identifying and penetrating terrorist cells. Similarly, the methods of identifying insiders who are providing information to adversaries are also firmly based in CI methods established during the Cold War. Modern technology can certainly augment these investigations and operations, but the basic approaches can be the same. The changes in how adversaries are using and exploiting IT systems, however, demand some changes to protective measures.

Active CI cannot be reserved for wartime or other periods of heightened threat. The CI Community needs to re-establish its role in protecting classified and sensitive information, not as a subset of security practices but as an equal partner. Cyber CI needs to be more aggressive in its use of deception. Advocates of an aggressive approach argue that there is an advantage to deliberately allowing the "attacker [to] gain access to information that is actually incorrect, thus providing incorrect intelligence and reducing the likelihood of the intensity of an attack increasing."<sup>27</sup> Although much has been written about the use of deception in warfare, it can be applied to peacetime operations as well, if used in a disciplined manner. The key is to align the CI mission with an intended effect.

Digital denial and deception can begin at the perimeter of a network, including the diversion of inbound probes to a simulated network that will respond with authentic but incorrect information.

The degree of sophistication of the simulated network should reflect the CI mission need. It will not deceive a sophisticated adversary, but may be a useful filter to help focus the attention of analysts on high capability threats. Critical infrastructure protection is one arena where ICS-type honeypots could be useful. Honeypots are “systems designed to be compromised by an attacker. Once compromised, they can be used for a variety of purposes, such as an alerting mechanism or deception.” A honeynet is a network of honeypots used “to learn the tools, tactics, and motives” of an attacker. Honeypots and honeynets are found most commonly as security research tools, typically as independent servers or networks that hackers attack at random. Observations from such research can identify the intentions or techniques used by the attackers, and the results are published on such community sites as the Honeynet Project.<sup>28</sup>

Similarly, the CI Community needs to think creatively about the information it protects and should engage in more red team analysis to identify information sources that could further the goals of an adversary. Moreover, engagement with the Infrastructure Protection Community must be re-established. When the U.S. Department of Homeland Security (DHS) was established, many infrastructure protection programs were transferred from the FBI, thus consolidating expertise on key issues and removing it from an agency with primary CI responsibilities. Although the FBI is still engaged in some infrastructure protection efforts, such as InfraGard, the unintended result of the transfer of critical-infrastructure-protection responsibilities to DHS is that infrastructure-related cyber incidents are handled reactively as criminal investigations. This limits the opportunity for the CI Community to engage with the Infrastructure Protection Community, which in turn limits the understanding of what the threats to the infrastructure are. Without active CI programs, the U.S. Government has little occasion to discover surreptitious activity to probe or penetrate U.S. ICSs. By investigating incidents primarily as criminal acts, opportunities to identify any but the least sophisticated adversaries are lost.

Without a more active CI strategy, the CI Community is at risk of being solely reactive and unprepared for future threats.<sup>29</sup> As time passes without more active engagement, the Community will miss important opportunities to identify how various foreign programs target U.S. networks and what their overall intent is. Some foreign powers, however, are beginning to identify how attacks on IT networks can be used innovatively in wartime. An examination of some of these writings—including the discussions of acupuncture warfare by the People's Republic of China (PRC)—can help reveal the threat that the United States may be facing.

#### ACUPUNCTURE WARFARE

As the United States keeps a close eye on its interests and allies in Asia, it must prepare for some form of friction with a China, whose expanding sphere of influence will increasingly overlap with U.S. interests, thus raising the potential for conflict.

Greater Chinese influence around China's periphery boosts China's regional and international power and influence and helps to secure an ambiguous world order; Chinese leaders seem more confident of China's power and influence but they also remain wary of and work against U.S.-led or other regional efforts seen as contrary to China's interests.<sup>30</sup>

Although globalization has linked the United States and China economically, socially, and culturally, the two nations are divided as to their political ideologies. The United States and China are likely to disagree on such issues as Taiwan, North Korea, and Japan that could spill over into conflict. In China's national security worldview, its security strategy is influenced by four features: a long border, many potential threats, a vulnerable domestic political system, and its view of itself as a great power.<sup>31</sup> In terms of cyber security, China presents a

potential threat with its continuing development of IW through technology, doctrine, and practice.

Chinese military writings describe a range of potential ways to implement IW. At one end of the spectrum is the *People's War*, inspired in part by Mao Zedong's philosophy. The concept is that IT allows all PRC citizens to participate directly in a conflict. Thus, with the largest population on the planet, it could be argued that China aims to bring this resource to bear by widespread attacks on U.S. networks.<sup>32</sup> Whether coordinated or uncoordinated, these attacks have the potential to cause disruptions in the U.S. information infrastructure. Past political conflicts between the United States and the PRC have led to heightened activity by Chinese hackers, but these have had relatively little effect, limited to Webpage defacements, denial-of-service attacks, and e-mail floods.<sup>33</sup> On the other end of the spectrum is a more sophisticated concept that would require intensive reconnaissance and coordinated execution.

Over the last few years, Chinese military theorists have referred to a concept called *acupuncture warfare*, which involves targeting key network nodes. The People's Liberation Army (PLA) has dedicated resources to develop, refine, and execute this methodology. Acupuncture warfare, based on attacking critical IT nodes or pressure points, capitalizes on optimizing effects on adversary vulnerabilities and follows the principle of acupuncture practiced for medicine—identifying points that serve as “a tunnel, or access route, to the deeper circulatory channels within.”<sup>34</sup>

One application of this theory would be finding the key choke points or supply chain vulnerabilities for U.S. military deployments and influencing them by attacking the supporting civilian infrastructure. In military conflicts, gaining the advantage of time can be as important as winning a battle. Causing an adversary's delay presents the opportunity for a *fait accompli* where the adversary was inca-

pable of intervening. Acupuncture warfare implies the ability to cause an effect in one part of the adversary (the military) by attacking a seemingly unrelated part (a rail line, communication system, or production plant). In this strategy, it is possible for an adversary to obtain pertinent military information and to act upon it by attacking private systems without ever penetrating or exploiting classified information or a secure network.

Regardless of the final strategy, it is clear that the PRC is investing in IW capabilities. U.S. analysts who have watched the PRC over time have observed that the Chinese “are devoting considerable time and energy to perfecting the techniques of IW to target rapidly modernizing Western armed forces that are becoming increasingly more dependent on the software that runs computer networks and modern communications.”<sup>35</sup> The PLA is bringing IW to prominence by providing IT training to its 1.5 million reserve force; it has also formed several IW regiments within its reserves.<sup>36</sup> The U.S. IC needs to closely monitor the development of China’s IW doctrine, which is clearly being designed with the world’s most technologically sophisticated military in mind. Lack of engagement with the Infrastructure Protection Community will leave the CI Community with little chance of knowing what the threat is before an attack occurs.

## CONCLUSION

As IT systems proliferate, the increased need for security is clear; the cyber environment, as described by the Office of the National Counterintelligence Executive, “provides unprecedented opportunities for adversarial activities and is particularly vulnerable because of the nation’s heavy reliance on information systems.”<sup>37</sup> The proper role for CI in national cyber security should not be subordinate to security activities, but partners with them, creating active CI programs that are charged with identifying the threat to specific types of networks as well as taking steps to neutralize them. Without these two activities, cyber

CI remains limited to providing vague warnings for foreign travel and reviewing incidents turned over from criminal investigations.

As mentioned above, the minimum involvement should go beyond incident management and damage assessments, to include advice on an organization's defensive posture, near-term IT acquisitions, and long-term enterprise architecture planning. Even this approach, however, limits the contribution that cyber CI can make to an organization. Too often, cyber CI is viewed as a completely separate endeavor from other CI activities, and neither informs nor is informed by incidents involving other types of adversary collection, such as open source collection, elicitation, and physical surveillance. Programs that do fuse such information have a much better sense of the adversary's intelligence cycle, as well as which foreign government offices have intelligence requirements, which direct collection, which collect, who analyses the information, and who ultimately consumes it. With this insight, a cyber operation can be truly effective, identifying the weak point in the adversary cycle and neutralizing or manipulating it. Regardless of whether CI efforts are prioritized by risk or threat, a mature program can identify the most urgent need and construct an adversary-specific strategy that involves both active and passive measures. This program can include partnering with appropriate federal agencies to target an individual in the adversary's intelligence process for U.S. collection, turning a foreign collector, or using deception to undermine the trust among collectors, analysts, and consumers. The latter takes careful planning, but deceptions do not need to be elaborate in order to succeed. Simple differences between the data that the adversary collects and what is later disclosed openly can subtly manipulate the adversary into questioning the value of the intelligence it receives or the quality or loyalty of the collectors. At its most potent, CI attacks the adversary's intelligence cycle through contamination rather than assault. As adversaries become more aggressive in the cyber realm, opportunities to exploit that collection blossom.

Clausewitz argued that war is not “the action of a living force upon a lifeless mass,” but the conflict between two forces hoping to achieve victory. The U.S. Government needs much more investment in detection and deception programs, using honeypots and related technologies to meet the threat and more aggressively counter it. Until the CI Community begins to react to the fundamental changes in the threat, it more closely resembles the lifeless mass rather than force hoping to achieve victory—and U.S. adversaries will have the advantage. The CI Community clearly needs a renewed commitment to innovation at the FBI, inside DoD, and within the Office of the Director for National Intelligence (DNI). These organizations should identify new approaches, new potential partners in the private sector, and new priorities within their areas of responsibility. The DNI should bring additional resources to bear on CI, use them as a coordinating and bridging mechanism to ensure that the various CI elements are sufficiently effective to identify the cyber threat and that they can work together to contribute to a coherent response. The investment to implement such a strategy is large, but it would match the enormity of the problem that the United States faces. The threat has fundamentally changed; the U.S. CI Community must acknowledge this revolution and make reciprocal changes that meet that challenge.

## Notes

1. Michael Warner, “Wanted: A Definition of ‘Intelligence,’” *Studies in Intelligence* 46, no. 3 (2002): pp.15–22. Note that the DoD definition of intelligence is “the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.” Defense Technical Information Center, Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 12 April 2001, as amended through 19 August 2009, p. 269.

2. For an in-depth discussion, see G.S. French, "Rethinking Defensive Information Warfare," 2004 Command and Control Research and Technology Symposium, 15-17 June 2004.
3. The Office of the National Counterintelligence Executive, National Counterintelligence Strategy of the United States of America, Office of the Director of National Intelligence, 2007, p. 9.
4. Defense Technical Information Center, Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 12 April 2001, as amended through 12 July 2007, p. 138.
5. Note that DoD removed the term "defensive information operations" from Joint Pub 3-13, Joint Doctrine for Information Operations, 2006, p. GL-7; although there is discussion of computer network operations and CI, there is no commonality between the missions in this latest version of the doctrine.
6. See, for example, the goals of the Comprehensive National Cybersecurity Initiative as described in John Rollins and Anna C. Henning, CRS Report R40427 "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," 10 March 2009, p. 6.
7. U.S. Government Accountability Office, Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing, October 2006.
8. Central Intelligence Agency, Office of Inspector General, "Report of Investigation: Improper Handling of Classified Information by John M. Deutch," (1998-0028-IG), February 2000.
9. W.S. Cohen and H.H. Shelton, "Joint statement on the Kosovo After Action Review," statement before the Senate Armed Services Committee, 14 October 1999, 106 Cong. 1 Sess; Dana Priest, "Serbs Listening in on NATO," *The Washington Post*, 1 May 1999, p. A1.
10. Transcript of Proceedings before The Honorable James A. Parker, United States Chief District Judge, United States of America, Plaintiff, vs. NO. 99-1417-JC Wen Ho Lee, Defendant, in the United States District Court for the District of New Mexico, 13 September 2000.
11. U.S. Department of Justice, Final Report of Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation, May 2000, (Declassified Version released 12 December 2001).
12. House Committee on Oversight and Government Reform, 110th Congress, "Interim staff report on Administration Oversight, White House Use of Private

E-mail Accounts,” 18 June 2007; R. Jeffrey Smith, “GOP Groups Told to Keep Bush Officials’ E-Mails” *The Washington Post*, 27 March, 2007, p. A3.

13. Charles E. Croom, Jr., “Guarding Cyberspace,” *Joint Forces Quarterly* 46, no. 3 (2007): p. 70.

14. Kevin R. Scott, Logistics Modernization in the United States Marine Corps: Materiel Distribution Center, Thesis presented to the Faculty of the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas 2005.

15. Blue force tracking refers to the “employment of techniques to actively or passively identify or track US, allied, or coalition forces for the purpose of providing the combatant commander enhanced situational awareness,” as defined in Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 12 April 2001, as amended through 19 August 2009, p. 69.

16. John A. Serabian, Jr., “Cyber Threats and the U.S. Economy,” statement before the Joint Economic Committee on Cyber Threats and the U.S. Economy, 23 February 2000, 106 Cong. 2 Sess.

17. The Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2007*. Office of the Director of National Intelligence, September 2008, p. 4; Defense Security Service, *Targeting U.S. Technologies – 2008*, U.S. Department of Defense, January 2009, p. 6.

18. The Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2005*. Office of the Director of National Intelligence, August 2006, p. 10.

19. Lawrence A. Gordon, et al. 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2005.

20. The Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2005*, p. 7; Defense Security Service, *Technology Collection Trends in the U.S. Defense Industry* (Alexandria, Virginia: U.S. Department of Defense, 2006), p. 5.

21. U.S. Department of Justice, U.S. Attorney, District of New Jersey, “Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing ‘Logic Bomb’ on Company Computers,” 17 December 2002, available from <http://www.usdoj.gov/criminal/cybercrime/duroniIndict.htm>, 22 Aug 2009.

22. Sharon Gaudin, “Case Study of Insider Sabotage: The Tim Lloyd/Omega Case,” *Computer Security Journal*, XVI, no. 3 (2000), pp. 1–8.

23. Eric J. Byres and J. Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE Congress, VDE Association For Electrical, Electronic & Information Technologies, Berlin, October, 2004.
24. Alan S. Brown, "SCADA vs. the hackers," *Mechanical Engineering* 124, no. 12 (2002).
25. The SANS Institute defines "war dialing" as dialing a block of numbers in an attempt to locate signals from modems or other data access points. See the 2006 paper "War Dialing," by Michael Gunn, available from [http://www.sans.org/reading\\_room/whitepapers/testing/war\\_dialing\\_268](http://www.sans.org/reading_room/whitepapers/testing/war_dialing_268), 22 Aug 2009.
26. Dana A. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat," Congressional Research Service, 20 January 2004.
27. John Davey and Helen Armstrong, "Dominating the Attacker: Use of Intelligence and Counterintelligence" in *Cyberwarfare*, School of Information Systems, Curtin University of Technology, p. 12.
28. *The HoneyNet Project, Know Your Enemy* (Boston: Addison-Wesley, 2002).
29. Melissa E. Hathaway, "Cyber Security: An Economic and National Security Crisis," *The Intelligencer* 16, no. 2 (2008): p. 32.
30. Robert G. Sutter, *China's Rise in Asia: Promises and Perils* (Lanham, MD: Rowan and Littlefield, 2005), p. 10.
31. Michael D. Swaine and Ashley J. Tellis, *Interpreting China's Grand Strategy: Past, Present, and Future* (Santa Monica, CA: RAND Corporation, 2000), p. 9.
32. Timothy L. Thomas, *Dragon Bytes Chinese Information – War Theory and Practice* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2004), p. 7.
33. "Military Forum," *Jiefangjun Bao (Liberation Army Daily)*, 27 July 1999, report obtained by e-mail from Mr. William Belk, 1 June 2000. Timothy L. Thomas. *Dragon Bytes Chinese Information – War Theory and Practice* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2004), p. 28.
34. Acupuncture definition available from <http://chronicfatigue.about.com/od/glossary/g/acupuncture.htm>, 22 Aug 2009.
35. Gurmeet Kanwal, "China's New War Concepts for a 21st Century Battlefield," *Institute of Peace and Conflict Studies*, no. 48 (July 2007): p. 4.
36. Thomas, p. 9.
37. The Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2007*, p. 9.

### Author Biography

Geoffrey S. French is the Analytic Director for Security Risk at CENTRA Technology, Inc., and currently supports a number of programs for DHS. Mr. French has worked in CI and the Critical Infrastructure Protection Community since the 1990s, supporting government agencies such as the FBI and DoD. Mr. French has designed a number of risk methodologies for DHS, including tools for assessing espionage risk, the terrorism risk to infrastructure, and all-hazards risk to a region. In addition to overseeing risk methodological development, he provides subject matter expertise in cyber CI, especially in policy and guidance. Mr. French has written a number of papers on threat and risk assessment and spoken at numerous conferences and academic settings. Some recent examples include: “The Challenges of All-Hazard Risk Management,” presented at the Defense Threat Reduction Agency, December 2008, and “Intelligence Analysis for Strategic Risk Assessments” in the December 2007 George Mason School of Law monograph *Elements of Risk*. He has a B.A. in History from Wichita State University and an M.A. in National Security Studies from Georgetown University. He is a founding member of the Security Analysis and Risk Management Association.

### Author Biography

Jin Kim is a Program Manager for CENTRA Technology, Inc., and currently supports strategic risk methodology development and analysis for DHS. Mr. Kim has broad and diverse experience in the security and intelligence communities—from tactical Army assignments to strategic assignments supporting DoD and DHS. He has a B.S. in Engineering from the United States Military Academy and an M.A. in Security Studies from Georgetown University’s School of Foreign Service. His recent co-authored publications include: *Threat Based Approach to Risk, Case Study: The Strategic Homeland Infrastructure Risk*

*Assessment (SHIRA)* presented at the Naval Post Graduate School, Monterey, CA; and *Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis*, published in the SAIS Review of International Affairs.