National Intelligence Estimate

The Global Cyber Threat to the US Information Infrastructure (U)

NIE 2009-03 REL FVEY

May 2009

NIC

[redacted]

US classified networks occasionally have been infected with malicious software over the years through the use of removable memory devices such as thumb drives or the forwarding of e-mail from unclassified to classified networks. As we have increased monitoring of US classified systems we have detected increased incidents of infection, but it is unclear whether this indicates a growing number of penetrations or merely increased observation of an ongoing problem. We also are uncertain whether any of these infections were intentional or if they occurred by accident.

- We assess with moderate confidence that adversaries probably will begin to adopt more resource-intensive tactics, such as taking advantage of insiders or introducing cyber attack vulnerabilities during the manufacturing stage of network hardware and software in the increasingly global supply chain, in order to counter the adoption of additional security techniques on targeted classified networks. (S//REL)

[redacted]

We assess with high confidence that **Russia and China pose the greatest cyber threats** due to their strategic interests and capabilities to target and disrupt elements of US and allied information infrastructures.

- **Russia** has a robust, multi-disciplinary computer network operations program with proven access and tradecraft and can conduct the full scope of operations, including computer network exploitation, computer network attack, insider-enabled operations, and supply-chain operations.

- **China** has become the most active foreign sponsor of computer network intrusion activity discovered against US networks but has not demonstrated the sophistication or range of capabilities of Russia. We assess with high confidence that **Beijing has dramatically expanded its level of effort in computer network operations over the past five years** and that China's state-sponsored information operations capabilities will continue to grow. Chinese cyber efforts include insider access, close access, remote access, and probably supply chain operations. Intrusion activity that we assess is probably sponsored by the People's Liberation Army has targeted US military and diplomatic organizations, defense

contractors, and companies and government organizations involved in deals of significance to Chinese industry. (S//REL)

[redacted]

We assess with high confidence that the increasing role of international companies and [redacted]

Confidence Levels for Key Judgments (U)

High Confidence (U)

- Almost all current and potential adversaries now have the capability to exploit and, in some cases, attack unclassified access-controlled US and allied information systems via remote penetration from the Internet. An increasing number of actors are seeking the capability to target the telecommunications system, secure systems, supply chains, and other components of the US information infrastructure.
- [redacted]
- Russia and China pose the greatest cyber threats due to their strategic interests and capabilities to target and disrupt elements of US and allied information infrastructures.
- The increasing role of international companies and foreign individuals in US information technology supply chains and services will increase the potential for persistent, stealthy subversions.
- [redacted]

Moderate Confidence (U)

- Adversaries probably will begin to adopt more resource-intensive tactics, such as taking advantage of insiders or introducing cyber attack vulnerabilities during the manufacturing stage of network hardware and software in the increasingly global supply chain, in order to counter the adoption of additional security techniques on targeted classified networks.
- [redacted] (S//REL)

Low Confidence (U)

- [redacted] (S//REL)

[redacted]

[redacted]

- [redacted]

- [redacted]

[redacted]

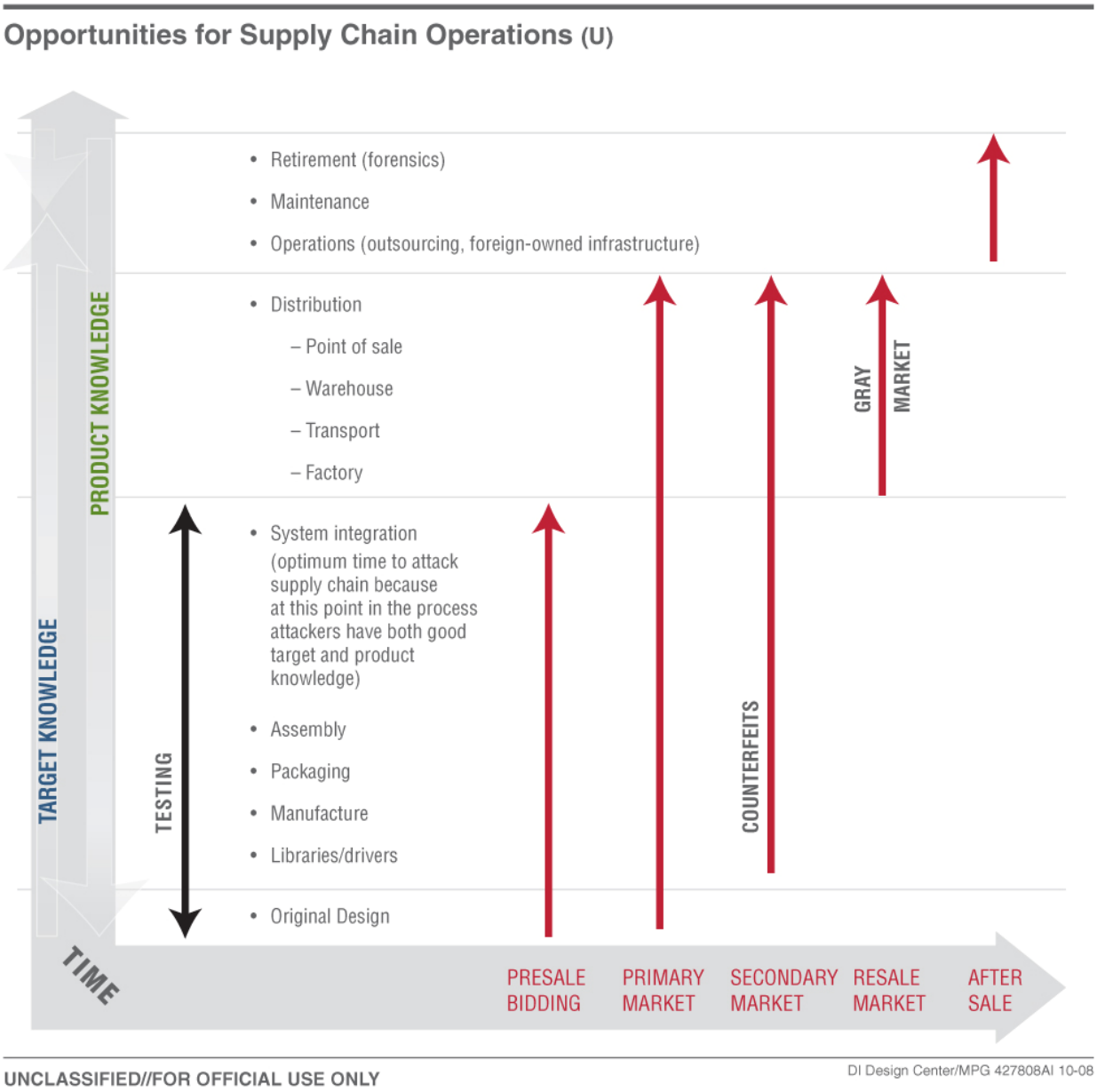
Cyber Supply Chain Threat Defies Easy Solution (U)

We assess with high confidence that the increasing role of international companies and foreign individuals involved in US information technology supply chains and services will increase the potential for persistent, stealthy subversions over the course of this Estimate. While foreign intelligence and military services are most likely to conduct supply chain operations, international terrorist and criminal groups or even companies engaged in industrial espionage could carry out such operations as well.

- Exclusion of foreign software and hardware components and products from sensitive networks and applications is already extremely difficult and will become more so as fully US-manufactured substitutes become increasingly scarce and US providers of cyber security products and services are acquired by foreign firms.

- Even if a successful exclusion policy could be implemented, opportunities for subversion would still exist through the use of front companies in the United States and adversary use of insider access in US companies. (S//REL)

In the event of a supply chain attack during a national crisis or wartime, US organizations may not have the means or the time to ascertain the trustworthiness of backup equipment and data. (S//REL)



Why Don't We See More Supply Chain Operations? (S//REL)

Considerable uncertainty overshadows our assessment of the threat posed by supply chain operations. Intelligence reporting provides only limited information on efforts to compromise supply chains, in large part because we do not have the access or technology in place necessary for reliable detection of such operations. This intelligence challenge is compounded by the unwillingness of victims and investigating agencies to report incidents. Many types of supply chain operations tend to be difficult and resource-intensive, however, and thus may not occur as often as the vulnerabilities of US systems might allow. (S//REL)

Threats to Electronic Voting (U)

On balance, we judge the threats of electronic vote tampering to be similar to those from traditional efforts to manipulate election results. Electronic voting machines are subject to many of the same vulnerabilities as other computers, such as software vulnerabilities, insider access, and supply chain threats, and numerous academic and government security examinations in the United States and other countries have discovered vulnerabilities in voting systems. We are unaware, however, of any attempts to use cyber attacks to affect US elections.

- The identification and exploitation of vulnerabilities in computerized voting systems by foreign cyber actors could undermine US democracy promotion efforts and support for pro-US opposition political parties abroad. (S//REL)

Influence of Technology Trends on Offense and Defense (U//FOUO)

Trends	Tradeoffs	Beneficiary
Network Convergence	• Convergence of telecommunications and Internet driven by economics. • Depending on implementation, particularly of signaling system, could leave telecommunications infrastructure vulnerable as Internet is today.	**Offense strongly**
Legacy Drag	• Expense of upgrading infrastructure hardware forces defense to work with old, less secure legacy equipment. • Forces designers to include backward compatibility, increasing chances that new equipment will inherit old vulnerabilities. • Defense seeks to avoid this through use of wireless infrastructure, creating new problems.	**Offense strongly**
Interconnectivity	• Offense has easier access to critical data, applications, and infrastructure. • Pervasive digital sensors provide offense the potential to subvert more critical systems, with greater potential for causing physical effects virtually.	**Offense strongly**
Wireless Communications	• Solves access problem for offense unless robust, secure, reliable protocols can be established.	**Offense strongly**
Unvetted Supply Sources	• As supply chains, particularly in the design phase, become more international, establishing trustworthiness of supply source more difficult.	**Offense strongly**
Programmable Hardware	• Allows defense to update or make real-time adjustments to hardware functionality, but software attacks could subvert hardware.	**Offense strongly**
Ubiquitous Media	• Use of common media such as USB drives on many types of devices and hardware creates a common vector for attack and data exfiltration.	**Offense strongly**
Device Convergence	• Small, portable, more powerful devices will be more attractive target. • Information associated with some device functions—sound, vision, and navigation—could be collected, used against owner. • Increasing power of devices will allow for security improvements, including call-home, encryption.	**Offense slightly**
Complexity	• More difficult for defense to build secure hardware and software. • Defense must "get it all right;" offense needs find only one flaw. • More difficult for offense to identify targets or reverse-engineer.	**Offense slightly**
Higher Bandwidth	• More data to collect but harder for offense to pinpoint its desired target.	**Neutral**
Outsourced Processing, Storage, and Security	• Systems used by defense to manage distributed processes and data will be new, potentially lucrative target, but centralized facilities could be protected. • Security as a service could increase security from intruders and obfuscate storage, but is dependent upon secure implementation and extends data access to insiders at outsourced services companies.	**Defense Slightly**
Virtualization	• Decreased risk to actual data and operating system. • Technology can also be applied to hide malicious files from the operating system, and virtualization applications could have their own vulnerabilities.	**Defense slightly**
Stateful security	• Techniques such as Deep Packet Inspection could improve defenders' ability to find compromises of computer as they occur.	**Defense slightly**
Optical Communications	• Fiber optic communications make intercept more difficult, present significant targeting and volume problems for offense.	**Defense strongly**
Cryptography	• Best defense to protect data, authenticate processes, particularly if includes hardware, multifactor authentication, and biometrics. • Offense will need to subvert people, supply chains, or implementation. • Can reduce the ability of defenders to conduct traffic analysis and inspection.	**Defense very strongly**

This table is **UNCLASSIFIED//FOR OFFICIAL USE ONLY.**

Outside Reviewers' Comments (U)

[redacted]

Dr. [redacted] *(U)*

(Continued on next page)

(Continued…) **Outside Reviewers' Comments (U)**

This NIE properly summarizes our knowledge and inferences on the cybersecurity threat. However, it may underestimate the vulnerability of our classified networks. A reasonable person may assume that any cyber operation the United States can perform against peer or near-peer countries, such as Russia or China, those countries could potentially perform against us. To the extent that we are successful in such operations, we should assume—absent compelling evidence to the contrary—that others may well have been successful against us. (S//REL)

Also, while the NIE properly identifies the insider threat as the major cyber threat, the Chinese supply chain may require additional consideration. The deep influence of the Chinese government on their electronics manufacturers, the increasing complexity and sophistication of these products, and their pervasive presence in global communications networks increases the likelihood of the subtle compromise—perhaps a systemic but deniable compromise—of these products. (S//REL)

Finally, it should be noted that even as our own computer network offensive capabilities are better developed than our network defense capabilities, the same may be true of our adversaries. Efforts to share information between offensive, defensive, and analytical cyber organizations should be encouraged to more fully inform the latter organizations of the magnitude of the potential threat. (S//REL)