~~SECRET//NOFORN//MR~~

Intelligence Science Board

(U//~~FOUO~~) Rapidly Advancing Globalization and the Emerging Threat of Foreign Information Operations: A Strategic Perspective

January 31, 2007

~~SECRET//NOFORN//MR~~

(U//~~FOUO~~) Rapidly Advancing Globalization and the Emerging Threat of Foreign Information Operations:

A Strategic Perspective from the Intelligence Science Board

(U) Summary

(U//~~FOUO~~) The Associate Director of National Intelligence for Science and Technology asked the Intelligence Science Board (ISB) to explore the impact of ongoing trends in the globalization of information technology (IT) on the future of foreign information operations (IO). The responding ad hoc ISB task force notes that foreign expertise in IT and IO is rapidly closing the gap with the United States in quality, if not yet in quantity. The task force therefore concludes that the U.S. Government should accept that any of its information systems and networks (even classified) may already be compromised, and, furthermore, that fully defending the global Internet against any and all attackers is impossible. Consequently, the task force recommends that the Intelligence Community adopt a more proactive strategic posture with regard to bolstering its information assurance practices, including surveilling its own networks, hunting for incursions, preparing viable contingency plans, and leveraging the knowledge and skills of the private sector and our offensive IO capabilities to advance the protection of all our systems. Further, the task force recommends that the Director of National Intelligence provide increased warning, advocacy, and leadership for a national initiative to better prepare all sectors of the nation for the age of cyber-based conflict.

(U) Preface

(U//~~FOUO~~) This report, prepared by the Intelligence Science Board, presents a strategic-level summary assessment of the impact of globalization on foreign information operations. The concurrently published companion ISB document, "The Impact of Globalization on Foreign Information Operations" [TS//SI//NF], contains a more detailed assessment of the threat and specific recommendations. The ISB study task force wishes to express its sincere appreciation of selected government personnel (identified in the larger report) who assisted the task force in understanding the history and extent of government approaches for addressing the issues raised in this study.

(b)(1)
(b)(3)

(U//~~FOUO~~) The emerging global threat from information operations

(U//~~FOUO~~) America is under attack; and the battleground is *cyberspace* – the highly technical domain of telecommunications, networks, computers, and digitized information. In this battlespace, the "weapon systems" are computers and the "warriors" are the software programs that they execute. At the same time, computers are also the *targets* of attack – attacks to disable information systems and the production systems they control, to modify critical information in an attempt to subvert decision making, or to steal information not otherwise available for military, economic, or other strategic or tactical advantage. This is the complex and emerging world of *information operations* (IO) addressed in this study.

(U) The United States, like all developed nations, relies increasingly on information technology (IT) in every aspect of government activity and citizens' private lives. Computers and digital processors control our transportation, entertainment, health care, banking, commerce, water and food delivery, government program administration, weapon systems, troop refurbishment, and intelligence collection, processing, and dissemination. *With this automation comes increasing vulnerability to cyber-based attacks* not only against the computer systems themselves but also, consequently, against the societal, business, and government systems they enable.

~~(S//NF)~~ [redacted]

[redacted]

~~(S//NF)~~ A related risk posed by the offshore production of IT (including microelectronics) resulting from globalization is the growing vulnerability of the United States to a reverse-International Traffic in Arms Regulation (ITAR) whereby *critical technologies could be denied to the U.S. in international trade.*

(U//~~FOUO~~) Where once our national security concerns focused on export control and on determining who was seeking to purchase American companies and technology, today we must be equally concerned about the *provenance* of the IT products we buy and the hidden capabilities they may introduce into our systems – capabilities that may be used against us. Thousands of times every day, cyber "warriors" attempt to penetrate our information systems. They do so to generate mischief, steal information, or put in place mechanisms that enable penetration or disruption of service at a time of their choosing.

~~(S//NF)~~ [redacted]

(b)(1)
(b)(3)

(S) Today such attacks occur continually against unclassified government, military, and commercial systems, as well as critical infrastructure systems in the private sector essential to our sustained national well-being. Of particular concern to the ISB task force, and less well understood, is the *degree of success these information attacks have achieved against our most sensitive systems and information.*[1]

(S//NF) [redacted]

(U) While experts debate whether or not a total collapse of the Internet and/or our national telecommunications system is technically possible, more subtle damage, with equally devastating results, is certainly feasible. The processes of both automation and globalization are viewed as largely *irreversible trends*. Maintaining information superiority is central to our national military strategy, and the economic and performance advantages of automation cannot be denied.

(U//FOUO) Similarly, increasing economic pressures to move manufacturing operations offshore and the global sharing of knowledge and information (largely enabled by the Internet) are irresistible and largely unstoppable. But the constantly improving IT capabilities of foreign nations, groups, and individuals carry with them a growing threat to our nation, our intelligence capabilities, and, ultimately, the ability of our intelligence customers to accomplish their missions.

(S) Concurrent with the globalization of IT has come a *globalization of offensive IO tools, techniques, and tradecraft*. Offensive IO capabilities no longer fall only within the purview of nation-state governments: they are readily available to insurgent groups, terrorist organizations, criminal elements, and even disgruntled or misguided individuals – some of whom may be insiders in sensitive organizations.

(U) The impact-power of cyber-based weapons is increasing as techniques emerge for using the target's own computers as unwitting agents for a strategic-level attack. Consequently, a relatively small and inexpensive initial operation can achieve a huge and widespread impact – a tremendous asymmetrical advantage that leads to what some have termed a new type of *weapon of mass disruption*.

(U//FOUO) The ISB task force concludes that the global propagation of offensive IO capabilities undermines current U.S. war-fighting and economic assumptions. We must bring our military, intelligence, and government planning and operations into the information operations age, and we have a long way to go.

[1] (S//NF) [redacted]

(b)(1)
(b)(3)

(U) The nation needs a more balanced approach

(~~S//NF~~) The nation, the government, and the Intelligence Community (IC) are, on the whole, insufficiently prepared to confront ongoing and potential foreign offensive IO effectively. We must update our **legal statutes** to recognize the threat from (and to) IT and the systems that IT enables. Our **policies** must be reshaped to permit (even demand) sharing of information among our own offensive and defensive IO forces – both to resolve potential conflicts and to better understand the global threat.

(U//~~FOUO~~) **Business practices** must be updated to help ensure that our systems always remain current with regard to best security practices and the installation of fixes to deter known attacks and to prepare for the eventuality that our systems have been and will be compromised. We must design national security **system architectures** from the start to anticipate deliberate malicious behavior (both internal and external). And our **intelligence priorities** must be refocused (and commensurately resourced) to address the growing and ever-changing threat of offensive IO against our national security and critical infrastructure systems.

(~~S//NF~~) [redacted]

(~~S//NF~~) We must find better ways to *share our knowledge about the form and extent of the threat* with those individuals and organizations upon whom our nation relies for defense against strategic or criminal attacks. Finally, we must *become ever more vigilant in monitoring the behavior and usage of our systems* to identify potential malicious actions while balancing the priorities of civil liberties and national security.

(U//~~FOUO~~) Terrorism and other threats raise the imperative to share information to unprecedented levels. At the same time, the huge community networks that we use for sharing (e.g., the Nonsecure Internet Protocol Router Network [NIPRNET], Secure Internet Protocol Router Network [SIPRNET], and the Joint Worldwide Intelligence Communications System [JWICS]) face unprecedented risks from the activities of sophisticated adversaries. The information assurance (IA) challenge for the next decade is to solve both problems at once: *the need to protect and the need to share.*

(~~S//NF~~) Hitherto, most national IA resources have focused on lower-end attacks, such as those mounted by hackers and the intruders who recently targeted NIPRNET. *Sophisticated* attackers operate using methods that are far more difficult to detect and more diverse in form, ranging from remote attacks, to insider subversion, to assaults on the supply chain.

(U//~~FOUO~~) Globalization has made IT supply chains increasingly vulnerable. Merely raising the IA bar will not suffice to defend against sophisticated threats. We must prepare and execute a broad portfolio of actions to transform IA and national security usage of IT in order to improve our defenses against sophisticated cyber threats.

(U//FOUO) Toward this end, the ISB task force offers the following suggestions for a coordinated IO/IA strategy for the IC:

- Install sound defensive business practices throughout the IC and ultimately the government;
- Take longer-term preventive measures, including building closer ties to private industry;
- Find and fool the adversaries in their offensive IO exploits before they do real damage;
- Develop effective contingency plans for when an adversarial IO attack *does* succeed; and
- Develop a comprehensive risk assessment approach to IO, IA, and IT globalization.

(U//FOUO) While aimed at strengthening the IC itself, this strategy can also serve as a model for other sectors of the government, industry, and our society. *The ISB task force encourages the Director of National Intelligence to provide increased advocacy and leadership in expanding this endeavor into a truly national initiative.*

(U) Install sound defensive business practices

(U//FOUO) Most important, the IC must maintain a vigilant defense and keep its information systems up to date with regard to the latest security patches, modern hardware developments, software upgrades, and sound business practices related to security. As basic as this concept would seem, economic and workload pressures often work against our keeping systems current. We must develop viable enterprise-level security strategies and enforce compliance. Many successful attacks on government agencies have been launched against *known* weaknesses in existing system software *after* vendors had already distributed effective patches, but before the agencies had installed them.

(S//NF) In the complex, interconnected world of cyberspace, we are each only as secure as the systems to which we connect (and they, in turn, as those to which they connect). One weak link in an otherwise strong network provides an opportunistic entry point for an effective and clandestine information operation – and yet, *we often do not maintain adequate records of system interconnectivity or component sourcing and history.*

(U//FOUO) **Patch existing systems and computers** as quickly as fixes are made available. Making security fixes must be mindful of operational impacts on complex legacy systems, but sophisticated adversaries need only a brief period or a cloud of confusion to insert their offensive IO wares.

(S//NF) **Strengthen existing IA architectures** so that they continue to support net-enabled (net-centric) operation while providing improved protection against a broader range of attacks. Substantial changes are needed to re-design systems to be more defensible. For example, such systems could feature controlled information sharing zones and the ability to contain infections, to degrade gracefully, to move selected data collections rather than controlling access, and to facilitate rapid reconstitution. More research is needed on the difficult problem of how to construct trustworthy systems from untrusted components.

(U//FOUO) **Greatly expand countermeasures against insider threats.** For

longer-term planning, the IC might achieve substantial improvements at moderate cost by taking advantage of emerging technology such as trusted platform modules and other vendor offerings. The IC must move quickly to assess the costs and benefits of these technological opportunities and to ensure better-protected supply chains for critical system components.

(U) Take other preventive measures and actively engage the private sector

(U//~~FOUO~~) Even if components and business practices are up to date, information systems that are not designed to anticipate adversarial attacks may suffer from a fundamental flaw that enables adversarial IO action. While protections remain necessary, the IC should beware the false sense of security conferred by "high fences" or "thick walls" (user authentication, intrusion detection, firewalls, and the like). The IC should also employ forward-looking surveillance to recognize potential attacks before they materialize. Toward this end, *the IC should engage the private sector, which invents, owns, operates, and provides most of the information infrastructure upon which the IC relies* – and which may already have substantial in-house capabilities for cyber-surveillance.

(~~S//NF~~) **Build upon leading-edge defensive IO strategies and techniques employed within selected private sector organizations.** Considerable expertise exists in the financial, telecommunications, and network management sectors. The IC can learn from what these organizations are already doing and from working collaboratively with them.

(~~S//NF~~) **Inform private industry about foreign IO threats and provide advocacy for addressing these issues.** Private firms, while possessing widespread technical expertise, may not immediately welcome government involvement. They may, however, not fully appreciate the breadth and depth of myriad adversaries' capabilities and intent with regard to IO – even operations targeted against their own organizations. *The IC needs a safe mechanism for reaching out to private industry and providing companies with relevant threat information.*

(~~S//NF~~) [redacted]

(~~S//NF~~) [redacted]

(~~S//NF~~) **Establish clear doctrine on the consequences of cyber attacks.** The best national strategy against cyber

(b)(1)
(b)(3)

threats is deterrence. Yet the United States currently places emphasis on reducing *vulnerabilities* rather than *threats*. Both initiatives are needed, but the latter requires a rich active-response portfolio and improved attribution capabilities to discourage an adversary from engaging in cyber threat activities.

(U//~~FOUO~~) **Rethink the process of acquiring national security systems.** National security systems, including platforms, armaments, intelligence, and mission support systems, rely increasingly on commercial components – precisely when increased globalization makes these components more vulnerable to foreign tampering. At the same time, national security systems are increasingly becoming network enabled, which provides a path for adversaries to access malicious components that might already be in place. Often such adversaries seek to make the system unavailable for use, yet in most cases the main IA goal within acquisition programs is to protect secrets rather than to ensure robust availability and integrity.

~~(S//NF)~~ [redacted]

(~~S//NF~~) To achieve the much-needed closer relationship between the IC and the private sector, **we will need national security carve-outs in the laws** to encourage and protect commercial interests when private firms help and cooperate with the government in all its forms. Changes in policy or even presidential directives may not suffice.

~~(U//FOUO)~~ [redacted]

(~~S//NF~~) Our intelligence systems, of course, have always been a target of espionage and foreign manipulation. Over time, the most visible espionage cases have involved access to computer-based files and information – often by *trusted insiders*. Passive mechanisms to prevent access are ineffective against the trusted insider who already has legitimate access, or the undetected intruder who is already inside our systems. [redacted]

~~(S//NF)~~ [redacted]

(U//~~FOUO~~) **Fund a robust research program** to develop defensive IO capabilities, including techniques for detecting, monitoring, defeating, and responding to intrusions.

(~~S//NF~~) **Greatly expand usage monitoring.** System usage monitoring is critical to improved information sharing.

(b)(1)
(b)(3)

This activity requires a near-term infusion of resources and action so that effective monitoring capabilities can be expeditiously developed and deployed.

(U//~~FOUO~~) Usage monitoring is invaluable when there are doubts about specific access authorization or where the policy in force is to share information liberally. In both situations, usage monitoring enables the enlightened information sharing policy of *trust, but verify*. Any policy on usage monitoring must also remain sensitive to privacy concerns, and maintain a careful balance between security and civil liberties.

(~~S//NF~~) Usage monitoring complements access control in other ways by enabling the Community to:

- Perform after-the-fact analysis of information sharing (e.g., to determine the impact when an adversary is caught exploiting collective legitimate accesses leading to increased aggregate risks);
- Detect abuses committed within a user's access privileges (e.g., trawling for large amounts of sensitive data unrelated to the user's current assignment);
- Keep a close watch on privileged users with extensive access rights (e.g., baseline their normal activity and scrutinize them closely when their activities fall outside the norm); and
- Counter sophisticated attacks that circumvent system access controls (e.g., usage monitoring of systems from which data might be exfiltrated to detect and possibly even prevent such attacks).

Usage monitoring will be improved by increased usage of *metadata tagging* of all digitized information.

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

~~(S//NF)~~ [redacted]

[redacted]

(U//~~FOUO~~) Develop effective contingency plans for responding to successful offensive IO attacks.

(U//~~FOUO~~) In the age of IO, it is naive to assume that critical information systems will always be available and reliable. Prudent operational planners develop alternative strategies to accomplish missions in the face of system fallibility.

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

[redacted]

(U//~~FOUO~~) Develop a risk assessment approach to offensive IO and globalization

(U//~~FOUO~~) Decision makers and system planners need better ways to identify and assess the risks inherent in our current and planned systems. Complex trades must be considered between system cost, system performance, and mission accomplishment, especially as IT globalization proceeds to cloud the meaning of "buying American."

~~(S//NF)~~ [redacted]

(~~S//NF~~) **Determine adversaries' capabilities and intent.** The nation must prepare itself much better for cyberconflict by gathering intelligence, counterintelligence, targeting information, and operations information. Decision makers must understand the potential for attacks on our civilian and private infrastructure to steal scientific and technical information, divert attention, gain commercial economic advantage, or generate public hysteria. [redacted]

[redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

[redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted]

[redacted].

(U) The IC needs a comprehensive, proactive IO strategy

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted].

(U//~~FOUO~~) We should also factor the potential economic impact of intellectual property losses into offensive/defensive IO equities. In fact, the need to protect and the need to share are natural partners that the IC should harness in an integrated team. We need defense in depth, both to enable information sharing and to provide robust protection against sophisticated adversaries. The IC can, and indeed must, meet both challenges.

(U//~~FOUO~~) The United States needs a national *wake-up call* and reality check regarding the global propagation of offensive IO capabilities. We must bring all government cyber activities into the IO age. We must develop IO-aware and IO-enabled strategies in coordination with policy and diplomatic initiatives. We must raise, across the government, the priority placed on developing national processes for response, damage assessment, and course-of-action planning for critical infrastructures.

(U//~~FOUO~~) Despite the negative implications discussed above, globalization can also present opportunities if we manage them correctly. The spread of technology is not limited to a single nation or entity, but occurs world-wide. As a result, *globalization can create a diversity of products and source options that can provide viable alternatives against single points of failure* and further complicate the mission of a cyber-attacker. To capitalize upon this "natural protection," however, U.S. Government purchasing needs to move from a large-scale, single-provider approach to a multiple-provider basis and seek a balance of cost efficiency versus security.

~~(S//NF)~~ [redacted]

(U//~~FOUO~~) Our national (and community) vulnerability to IO does not result from globalization, but is exacerbated by the instantaneous advancement of knowledge and skill around the globe. If not addressed, the relentless march of globalization will further close the gap between U.S. technological superiority and the skills of other nations. *There may come a day when our indigenous technical capability is inadequate to respond quickly enough to a cyber attack.*