Information and Communications Technology and the Global Marketplace

The DoD Globalization Task Force Staff

The global information and communications technology (ICT) marketplace brings innumerable benefits to the USG and DoD. However, this extended and often unknown supply chain has created an environment where trustworthiness in commercial ICT products is no longer implicit, requiring the USG to expand its understanding of IA. In this new environment, employing comprehensive protection mechanisms requires consideration of both the depth and breadth of the approach; that is, risk and risk mitigation must be considered across the entire lifecycle of the product or system, from requirements development to retirement. The DoD is working to develop solutions to manage risk at the network, systems, and product level. Potential solutions include partnership with industry in supply chain oversight and standardization to facilitate keeping intruders and malware out of USG and DoD networks.

The impact of the global marketplace on USG IA activities and technology acquisitions is permanent, irreversible, and likely to have only greater impact over time. In order to stay on the cutting edge of technology development, the USG and its commercial supplier base must rely on industry partners from around the world. And, with increasing frequency, it is foreign companies that are providing the most advanced technology solutions. The multi-tiered, global nature of our supply chain means that the government has suppliers that it may not know and may never see. With less insight into their security practices and less control over how they conduct their business, this global supply chain may make the USG more vulnerable to an adversary who can use security gaps in our global supply chain against us.

Our traditional defense approach, *defense-in-depth*, as defined by DoDD 8500.01E, focuses on the following:

> ... establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among information technology assets; and, the selection of IA solutions based on their relative level of robustness. [1]

This approach implies a degree of trustworthiness in commercial ICT. However, trustworthiness in commercial ICT products is no longer implicit. A new defensive strategy, *defense-in-breadth*, is necessary to complement our traditional approach and manage risk over the lifecycle of a network, system, or product.

The comforting assumptions the DoD and the broader USG have had about their suppliers are no longer true – especially in the ICT industry. No industry has been more transformed by globalization than the ICT industry. Today, ICT – including micro-electronics [2] and software [3] – is being developed around the world. Companies may be headquartered in the United States but perform much of their research and development, manufacturing, and servicing in China, India, or numerous other countries. In addition, these companies contract out work to multiple subcontractors whose processes and practices are often unknown. Even for the decreasing number of ICT firms that are largely based in the United States, much of their talent may come from abroad.

... with a much more transitory, global, and permeable supply chain, trustworthiness in our ICT is no longer a guarantee — even from our American companies.

This picture of a truly international industry contrasts sharply with the supplier base that the DoD and other USG agencies dealt with in the past. They were able to count on companies here in the United States with domestic research, manufacturing facilities, and American employees. Moreover, the government could be confident that these *all-American* companies were developing the cutting-edge technologies that underlay so much of American strategic dominance. These were firms whose products they could trust. However, with a much more transitory, global, and permeable supply chain, trustworthiness in our ICT is no longer a guarantee – even from our American companies.

There is no way to go back to a supplier base of all-American companies. While some departments do, for extraordinary reasons, build proprietary technology for government use using a cleared facility and cleared personnel, this approach is neither ideal nor financially feasible on a large scale for the bulk of the purposes for which ICT is intended. Business practices and the worldwide development of technology make the old ways impossible.

First, globalization optimizes resource use and improves the efficiency of production and distribution. Now, a team of developers in California can stop work and hand off their project to a team in Europe, which can, in turn, hand off to a team in Asia – making for a 24-hour development day. Moreover, those foreign developers are highly competent, are able to provide insight into the requirements of foreign markets, and can produce a competitive advantage in the U.S. market.

Also, the supply chain itself complicates the USG's ability to ensure the trustworthiness of products purchased from the global marketplace. Lean manufacturing processes and just-in-time operations exacerbate the lack of control, limit transparency, and inhibit the ability to inject security into the process. In a highly competitive environment, security testing may be minimized because the cost and time required are hard to absorb.

The national security concern regarding the global marketplace is that software or microelectronic circuitry may include deliberately inserted malicious logic – *malware* – that an adversary might slip into a

computer system to steal or corrupt data or disrupt the system. The malware might act immediately or it may be designed to lie dormant until activated by some future signal. Buried in the millions of lines of code that comprise the modern computer application, such malware is difficult to detect even with desktop-level malware applications such as Symantec: no one may be aware of its existence until after the damage is done.

For example, it was reported in Britain's *Channel Register* in November, 2007 [4] that hard-disk drives built for a U.S. data storage company by a Chinese subcontractor were infected with a Trojan horse virus named AutoRun-AH, which searches for passwords to online games and sends them to a server located in China. Although the company acted promptly upon the discovery of the malware, some units were sold to the public before it became aware of the compromise.

While compromising ICT may not be as easy a way to penetrate a computer system as hacking into it or turning an insider, it is a viable option for a determined adversary. Moreover, to the extent security measures make hacking more difficult or subversion more challenging, infiltrating the supply chain becomes a more attractive alternative.

There is no single – nor quick – fix for mitigating the risk to DoD and USG systems and networks stemming from the global ICT marketplace; yet the problem is not an impossible one to manage through a defense-in-breadth. The risks associated with a globalized supply chain can be addressed if one understands the problem, makes a concerted effort to address threats and vulnerabilities at key points over the life of ICT products and systems, and partners with commercial providers to improve the integrity of ICT products. Depending on the level of risk to the system or network, the mission area, and available capabilities, different systems and networks will require different combinations of risk management techniques. For national security computer systems, that effort is, therefore, going to be far more extensive than for another buyer with a less sensitive system – the challenge for any user is to select a mix of options that is cost-effective.

Both suppliers and acquirers have to be aware of the risk. Many government agencies and companies are beginning to rethink the implications of globalization on their supplier base. Neither they nor the sellers may have been sensitive to the possibilities of supply chain vulnerabilities in the past. No one is going to act unless they understand that there is a problem, and that level of awareness is only now developing.

One useful step will be for ICT suppliers to develop and maintain practices and procedures that monitor the development process in both their own facilities and those of any subcontractor that they use. Processes and tools that track when source code or hardware is accessed, who accesses it, and what changes they have made raise confidence. Similarly, strong business processes managing reputability and quality of components incorporated into ICT help bound risk. Commercial standards in this area clarifying commercial best practice regarding configuration management, design, and quality control in the presence of global sourcing can enable the systems' acquirers to express requirements and bound risk that unanticipated code or components have been placed within a reputable developer's configuration.

Buyers and testing labs have tested the functionality of software and hardware for many years — ensuring it does what it promises — but they have not been as focused on testing for security.

The adoption of such standards and best practices will proceed only if acquirers recognize their importance, require that suppliers adhere to these security processes, and recognize that a low-cost, low-security supplier can present a much higher cost in the long run. Those with the knowledge to create standards will likely do so only if there is genuine pressure from the larger buyer community to get it done.

However, at the time of purchase, a user may face a troublesome reality: even for those that have adopted all the standards and best practices required, there is no complete assurance that the product is trustworthy. Here, users must be more vigorous and sophisticated in protecting themselves. They have to evaluate the residual risk arising from the ICT that they are about to purchase and decide what steps they can take to configure their own systems to minimize that risk. The financial industry and some government agencies have been developing best practices to employ to counter this residual threat. The practices are tailored to the level of risk and the importance of the system, but the challenge will be to adapt enduring security controls in light of continuous technology changes, such as software updates, and shifts in an adversary's tactics.

One might ask if the entire problem could be solved by simply testing all that code to see if it contains malware. That is easier said than done. Buyers and testing labs have tested the functionality of software and hardware for many years – ensuring it does what it promises – but they have not been as focused on testing for security. It has traditionally been easier to test functionality than security, and the gap between the two has only grown as applications have become more complex. Even if the problem could ultimately be solved by testing, no such test is currently on the horizon. In its September 2007 report on Mission Impact of Foreign Influence on DoD Software, the Defense Science Board (DSB) recommended that the DoD fund science and technology research and development in state-of-the-art software and hardware vulnerability detection and mitigation [1]. The DSB highlighted the desired outcomes of this R&D as developing technology to eliminate accidental vulnerabilities from systems development and to improve trusted computing group technologies to mitigate the risks posed by malicious software [5].

The Cyber Security Research and Development Act (CSRDA) of 2002 [6] is one possible means of supporting the development of better tools. The CSRDA was signed into law November 27, 2002, to enable the U.S. to prepare against cyber-attacks on federal and private computers. The act directs the National Science Foundation to establish cyber-security research centers, community college grants, fellowships and undergraduate program grants, partnerships with industry and academia, and the establishment of a program to encourage senior researchers in various fields to transition to work in computer security [7]. The CSRDA authorized more than $900 million over five years for R&D and

training programs by the NSF and the National Intelligence Support Team. However, it is not clear how much time and money it will take to create new tools – and there is no guarantee that they will be able to keep up with the continually increasing complexity of the products they are reviewing.

There is one thing that is not part of the solution. There is no value in simply *banning* software or hardware manufactured in any particular country. Such a ban assumes that somehow the problem is geographically focused. It is not. Such a ban would not only raise questions under the rules of the World Trade Organization, but would also disrupt the ongoing operations of numerous legitimate U.S. and foreign companies that have come to rely upon work products from various overseas resources. Moreover, it would give a false confidence to buyers who might assume that merely because a product was produced in the U.S., for example, it should be secure.

Instead, the USG must reach out to global commercial partners to improve the state of play. Government cannot solve the problem without industry's help, and industry stands to benefit from dealing with the problem of supply chain risk in many ways. ICT providers need to be able to assure all of their customers, not just those with national security concerns, that the product being provided is genuinely secure. A widespread fear among buyers that there might be malware in their new software, for example, would depress sales and tarnish a brand. One only need recall the recent problems with lead paint on toys from China to understand the potentially devastating impact of a malware scare on software products.

An analogous problem facing commercial ICT developers is the reliability concern stemming from the increasing circulation of counterfeit commercial components. The globalization of the marketplace has led to commercial collaboration among widely diverse cultures, including those for whom respect for intellectual property is an emerging concept. This situation has led to a significant problem of counterfeit ICT component parts and products, often developed without quality or security best practices, appearing in critical systems and networks.

The heightened awareness of more general security issues associated with the Internet and software has led to increased emphasis on information security. Increased use of intrusion detection devices and other controls will likely have some benefit with regard to supply chain risks as well as those that come from more typical problems such as hacking, but more must be done.

The DoD is committed to managing the risk presented by globalization using defense-in-breadth: a multi-faceted, risk-mitigation strategy that seeks to identify, manage, and eliminate risk at every stage of the IT system or network lifecycle, from system requirements generation to system retirement. It is actively working to ensure that policies and processes are put in place to raise awareness of the risk, empower acquirers to make informed decisions when they request and procure ICT products and services, and arm acquirers with practices and tools necessary to mitigate risk when ICT products are used across the government (the more traditional defense-in-depth component). It is also partnering with the commercial companies that comprise its supply chain and using its power as a consumer to drive security-minded attributes into the development and management of new systems and technologies. Both government and industry stand to lose if the risk presented by globalization of the ICT supply chain is not managed effectively. Our adversaries' exploitation of vulnerabilities in the ICT supply chains have the potential to threaten our national and economic security by putting sensitive USG and corporate information at risk and generating distrust in the security of ICT products. The DoD cannot solve this problem without help from its partners both in government and industry.◆

References

1. Department of Defense Directive 8500.01E. "Information Assurance." 24 Oct. 2002 <www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>.
2. Defense Science Board. Report of the Defense Science Board Task Force on High Performance Microchip Supply. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Feb. 2005.
3. Defense Science Board. Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Sept. 2007.
4. Leyden, John. "Chinese Trojan on Maxtor HDDs Spooks Taiwan." Channel Register. 12 Nov. 2007 <www.channelregister.co.uk/2007/11/12/maxtor_infected_hdd_updated>.
5. Defense Science Board. Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Sept. 2007.
6. Pub. L. Cyber Security Research and Development Act. Nov. 2002.
7. GovTrack.us. "H.R. 3394 107th Congress (2001): Cyber Security Research and Development Act." GovTrack.us <www.govtrack.us/congress/bill.xpd?bill=h107-3394>.

About the Author

Mitchell Komaroff leads and is the Acting Director of the Globalization Task Force (GTF), for the ASD(NII)/DoD CIO. The GTF is an office within the Office of the DoD CIO dedicated to strategic national security planning to address risks arising from the globalization of the telecommunications infrastructure and of the marketplace for information and communications technology. He is primarily responsible for developing and implementing a strategy for mitigating national security risks to DoD arising from the increasing globalization of the ICT sector. The GTF is the ASD (NII)/DoD CIO focal point for transactional risk management in Committee on Foreign Investment in the U.S. and Federal Communications Commission licensing matters, developing strategies for preserving and improving Internet security and stability in support of DoD and USG communications, and policy development addressing global supply chain risk. Komaroff has worked to implement software and systems assurance across the DoD. He has worked previously as a computer scientist with DISA, and with industry where he worked network quality of service, IA architecture, and information management issues. Komaroff holds a master's degree in mathematics from George Mason University and a Juris Doctor degree from the University of Maryland, School of Law.

Phone: (703) 697-3314
E-mail: mitchell.komaroff@osd.mil

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government