COUNCIL *on* FOREIGN RELATIONS

CYBER BRIEF

Improving Supply-Chain Policy for U.S. Government Procurement of Technology

Danielle Kriz
October 2015

This Cyber Brief is part of the Digital and Cyberspace Policy program.

Policymakers around the world are increasingly concerned about the security of information and communications technology (ICT) supply chains. As governments rely more on ICT to conduct services, they worry about the proliferation of counterfeit products and malicious code, as well as the growing number of cyberattacks on these ICT systems. Within this context, governments are demanding that vendors improve the security of ICT products sold to the government, with a particular focus on vendors' supply chains.

Some recent policy proposals, however, threaten to do more harm than good. When developing supply-chain risk management policies, policymakers should ensure they address clearly identified gaps, build on existing best practices, promote solid risk management practices, work globally, improve the government's own ICT procurement practices, and facilitate more actionable cyber-threat information sharing with affected vendors. In addition, U.S. trade negotiators should discourage discriminatory, country-of-origin-focused prohibitions emerging from China and India. Failing to do so will harm the competitiveness of U.S. ICT firms.

BACKGROUND: GOVERNMENT SUPPLY-CHAIN POLICIES ARE MULTIPLYING

Governments increasingly rely on commercial off-the-shelf technologies to run sensitive government functions and hold citizen data. At the same time, ICT is becoming more complex and often more vulnerable to a growing number of cybersecurity threats. Governments are worried about the risks of procuring counterfeit ICT products or products containing malware, and are finding they have less visibility into companies' complex ICT supply chains.

Within this context, U.S. policymakers have proposed or enacted policies on vendors' supply-chain cybersecurity. There have been dozens of related bills and provisions in legislation, including in successive National Defense Authorization Acts, continuing resolutions, and omnibus appropriations bills. The Department of Defense (DOD), Department of Homeland Security, National Institute of Standards and Technology (NIST), Office of Management and Budget, and General Services Administration (GSA) all have worked on supply-chain cybersecurity. Even the Federal Energy Regulatory Commission has gotten into the game, issuing a notice of proposed rulemaking regarding "the development of standards for supply-chain management security controls to protect the bulk electric system from security vulnerabilities and malware threats."

The proposals and activities take different tacks. Some focus on partnering with industry, take global approaches, and acknowledge that risks and threats cannot be completely eliminated—only managed. Unfortunately, there is also a plethora of worrisome approaches—proposals that ignore the global nature of today's ICT supply chains, where hundreds of suppliers based in multiple countries provide the hardware and software that compose a finished product.

Examples include requirements that ICT vendors use certain product development technologies. In 2013, a DOD bidding process proposed requiring its software vendors to use a particular vulnerability-detection technology. Other regulations exclude or scrutinize vendors based on where or by whom a product is made. Certain U.S. laws, such as a section of the January 2014 appropriations bill, single out countries by requiring government purchasers to conduct added scrutiny of ICTs produced by companies "owned, directed, or subsidized" by China. Other policies give intelligence agencies and DOD the power to exclude vendors from procurements without notice due to "national security concerns" and also prevents them from informing the vendors about suspected supply-chain risks.

While most policy activity is in the United States, it is not acting alone. India's "preferential market access" policies, launched in 2013, direct government agencies to give procurement preferences to ICT vendors relying on Indian-made content. Some Indian officials admit they aim to force companies to put supply chains in India, stating that products made there are more secure. In September 2014, China released plans requiring its banks (which are state owned) to ensure that 75 percent of their ICT products are "secure and controllable" by 2019, to reduce their reliance on foreign ICT equipment.

SECURITY AND TRADE CHALLENGES

Whereas the ostensible policy objective—improving cybersecurity—is legitimate, legislating solutions can often do more harm than good.

First, some approaches decrease security. Policies mandating certain technologies, standards, or practices cannot keep up with threats that evolve constantly and affect each firm uniquely. A check-the-box compliance regime will likely deter firms from responding to risks for fear of violating a regulation, and divert resources from where security is needed and from developing responses to new risks. Mandated practices or technologies also benefit adversaries who, knowing the defenses employed, can circumvent them. Finally, if the government cannot inform vendors about identified supply-chain risks, vendors will not know about or be able to mitigate them. Keeping vendors in the dark on known risks can implicate security for all their customers.

Country-of-origin requirements also hurt security. The integrity of software development processes and procedures to detect the introduction of counterfeit products and malware into supply chains has a larger effect on product security than the location of a facility. In fact, a 2012 General Accountability Office study found that tracking an ICT product's country of origin provides "minimal security value relative to cost."

Second, many policy proposals duplicate or undermine existing risk management processes in government and industry. Within the U.S. government, NIST and other agencies collaborate with the public and private sector to research, develop, and share supply-chain risk management tools and practices. Many firms develop and employ secure product development practices and stringent supply-chain controls to improve their competitiveness. Global efforts to develop voluntary supply-chain risk management standards and best practices are found in various forums, such as the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). Many congressional proposals also fail to leverage these activities.

Policies mandating specific supply-chain practices to satisfy the U.S. government hurt the global competitiveness of U.S. firms. This competitiveness stems largely from developing leading-edge, affordable products—made possible by using complex, geographically dispersed supply chains. Globalized supply chains improve access to talent and high-quality, low-cost inputs and allow for resiliency, proximity to suppliers, and economies of scale. Diverting resources to meet U.S. government–specific requirements negates these benefits because companies must build tailored products in addition to global product lines. Given that many ICT companies, including U.S. ones, sell a significant number of their products to non-U.S. consumers, this raises costs, draining resources from research and development. Although the U.S. government is not a major market for all ICT companies, it is for some, and its ICT procurement policies have trickle-down effects on the entire tech industry.

Country-of-origin requirements invite copycat provisions or retaliation, raising market barriers for all firms. They also compound challenges U.S. firms face in foreign markets since former

National Security Agency contractor Edward Snowden revealed some firms' complicity, often unwilling, in U.S. intelligence efforts. Although the author of the 2014 appropriations bill language that mandates additional scrutiny of ICT products connected to China admitted his target was Chinese vendors such as Huawei, U.S. companies have struggled in selling their wares to the U.S. government since nearly all ICT has a "connection" to China. In addition, the provision has emboldened other governments to create their own national supply-chain requirements. The Chinese government has pointed to the 2014 appropriations bill to justify its own discriminatory policies, such as the "secure and controllable" banking regulations; India used it as an excuse for its market access policies.

RECOMMENDATIONS

The U.S. government should support the development and voluntary adoption of industry-driven standards instead of setting unique requirements. Better approaches are found in NIST, which has a long history of partnering with industry and playing a convening role on cybersecurity issues, as exemplified by its development of standards and guidelines for the protection of federal ICT systems and the agency's success developing the Cybersecurity Framework, a voluntary risk management tool embraced by many economic sectors. The Software and Supply Chain Assurance Forum, cosponsored by DOD and others, is another public-private partnership effort. In addition to leveraging industry activities, government policies should avoid duplication and be globally workable.

The government should also improve its own ICT procurement practices. This includes ensuring effective implementation of GSA's and DOD's February 2013 mandate to improve cybersecurity in federal acquisition planning and contracts. A recommendation from their November 2013 report is critical: federal purchasers and contractors should procure equipment directly from authorized sellers or resellers. There have been cases of government agencies buying ICT outside of authorized channels, such as via auction websites, only to acquire counterfeit or tainted products.

In addition, U.S. policymakers should help the private sector protect itself against threats by facilitating more actionable cyber-threat information sharing, including informing vendors when intelligence agencies find vulnerabilities in supply chains or products. Affected vendors need specific, targeted threats and technical indicators so they can take appropriate measures to protect and defend their supply chains. Policymakers should ensure effective implementation of Section 4 of Executive Order (EO) 13636 as well as EO 13691. Congress should pass cyber-threat information-sharing legislation to address liability concerns impeding greater information flows. The privacy concerns raised by some opponents can easily be mitigated through appropriate legislative language limiting sharing to threat indicators used for cybersecurity purposes.

Finally, U.S. government cybersecurity experts and trade negotiators should continue to discourage China, India, and other governments from enacting discriminatory supply-chain security policies lest a race to the bottom of country-specific policies ensue—a dangerous outcome that threatens the cybersecurity of ICTs and trade globally. The policy approaches recommended above will bolster the efficacy of any U.S. argument in this regard, underscoring yet another reason why the United States needs to get its supply-chain security policies right.

About the Author

Danielle Kriz is a cybersecurity fellow at the New America Foundation. Formerly the director for global cybersecurity policy at the Information Technology Industry Council (ITI), she founded ITI's cybersecurity policy practice. She has worked in Silicon Valley creating government affairs strategies for high-tech firms, and previously spent a decade in the U.S. executive branch developing and negotiating the government's high-tech trade policies at the U.S. Department of Commerce and the U.S. International Trade Commission. She has worked on cybersecurity policy for thirteen years and focuses on the intersection of cybersecurity, innovation, and international trade. She has been active in shaping cybersecurity policymaking in the executive branch and Congress, as well as for the European Union (EU) and EU member states, China, India, Japan, South Korea, Brazil, and others.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.