Mark Foulon and Christopher A. Padilla

In Pursuit of Security and Prosperity: Technology Controls for a New Era

The forces of globalization have created historic opportunities for human progress but have also spawned threats of terrorism and proliferation of weapons of mass destruction (WMD). As barriers to the flow of people, products, capital, and information lower and change in nature and scope, national security policy and economic policies are becoming increasingly intertwined. As a consequence, policies once seen as primarily security related, such as nonproliferation, defense sales, and border protection, now have important implications for economic policy. At the same time, issues typically in the area of economic policy, such as foreign direct investment, tax, and visa policy, increasingly have security implications. The controversy over the purchase of U.S. port operations by a Dubai-owned company in early 2006 and the current debate over immigration policy are but two examples of this emerging reality.

The complex relationship between economic and national security interests is nowhere more evident than in the area of technology collaboration—U.S. business's conduct of technology trade, research and development, and manufacturing with and in other countries. The advances in composite materials technology that come out of U.S. laboratories for use in making commercial aircraft stronger and more fuel efficient could also end up making the fighter aircraft of potential adversaries more deadly if a coproduction agreement with a foreign company were to go wrong. The latest developments in nanotechnology could threaten U.S. security if diverted through leaky research and development collaboration to improve the performance of a rogue state's missiles. In this dynamic world, U.S. policymakers must strike the right balance of controls, incentives, and market-based policies to allow the United States to reap

Mark Foulon is acting undersecretary of commerce for industry and security. Christopher A. Padilla is assistant secretary of commerce for export administration. The views expressed are not necessarily those of the U.S. government.

the benefits of technology collaboration while minimizing its potential threats to national and economic security.

Balancing Opportunity and Security

Three changes generally grouped under the rubric of globalization have significantly altered the calculus for decisions involving national security and economic interests in general and specifically for those concerning controls on technology collaboration. First, recent decades have witnessed dramatic increases in the cross-national flow of capital, goods, and knowledge as countries around the world have embraced free markets. This phenomenon has created billions of potential customers for U.S. products and millions of new competitors. Notably, India and China are on the rise as global stakeholders. U.S. firms face an ever-growing challenge to operate profitably in a hypercompetitive global marketplace.

The geopolitical landscape also continues to change dramatically. Nearly two decades after the fall of the Berlin Wall, the impacts of the end of the Cold War are still rippling through the international system. No longer divided into two blocs, today's geopolitical and economic environment has grown far more complex, as any one economy could be home to a mix of proliferators, terrorists, and legitimate customers. As transnational actors and movements, both benign and deadly, become more prolific and influential, governments cannot necessarily control present and future perils. As they demonstrated in their deadly attacks on the Madrid railways in March 2004 and the London subway in July 2005, terrorists can strike even at the heart of the United States' closest allies.

Finally, the technological revolution, like all such upheavals, brings progress and pain. Today, people throughout the world enjoy capabilities undreamed of a generation ago. Rapid declines in communication and transportation costs have changed business models and created opportunities for new enterprises. Instead of looking for a pay phone, teenagers can use their cell phones to call, text message, or e-mail their friends, all while surfing the Web or downloading a song from their favorite artist. Their parents think nothing of popping a CD into the Asian-made player using infrared laser technology in their automobile that was built from parts manufactured in Japan, Canada, and the United States and delivered just in time to the factory floor in Kentucky.

Advances in technology, however, have also led to new and deadly threats. The same Internet services that allow families to call long distance for the price of a local call also permit terrorists to download the blueprints or details of critical infrastructure systems. From terrorist attacks at home to the spread of weapons of mass destruction abroad, from the rapid mobility of global dis-

eases such as SARS to breaches in cybersecurity, the era of globalization is marked by profound new threats to U.S. security from technological innovations. For example, U.S. and coalition forces fighting in Iraq and Afghanistan have been killed by improvised explosive devices activated by the latest cell-phone technology. A rogue scientist such as Pakistan's A. Q. Khan can use just-in-time global shipping networks to provide illicit nuclear technology to outlaw nations.

> If U.S. technology controls are too restrictive, foreign competitors will readily fill the void.

As President George W. Bush wrote in his introduction to the 2002 National Security Strategy of the United States, "the gravest threat our nation faces lies at the crossroads of radicalism and technology." These trends of growing economic interdependence and competition, geopolitical change, and technology innovation make the control of the transfer of technology across borders more challenging and the threats posed by the exploitation of sensitive technologies more acute. To sell advanced technology products to a foreign purchaser, for example, a U.S. manufacturer may sometimes design or produce parts of those products in the country of the purchaser. That country, however, may have a military program the United States does not wish to support or have weak controls that raise the risk of diversion of sensitive technology into the wrong hands. Technology controls must be able to facilitate legitimate and necessary collaboration while safeguarding those products. At the same time, if overly restrictive technology controls deter U.S. firms from responding to market demands, foreign competitors will readily fill the void, costing U.S. firms sales, profits, and global leadership in industries that are critical to U.S. security.

Building Blocks for Technology Collaboration

Although the current system of controls does meet existing U.S. national and economic security needs, the speed of twenty-first-century globalization compels innovation and compels it quickly. Controls that work for trade-based technology collaboration may not work as well for processes that involve knowledge production and dissemination, such as coproduction or research and development. Trade, the shipping of a physical product from a producer in one country to a customer in another country, is the most basic and common type of technology collaboration, and trade controls are relatively straightforward. After an evaluation, an export proceeds with or without conditions or not at all. If a product were illegally diverted, it could be used by an unintended consumer, but absent reengineering, the design and production knowledge stays with the manufacturer.

When technology collaboration involves the transfer of knowledge as well as products, however, the complexity of the control process must increase. The sophisticated know-how required to assemble disparate components into a commercial aircraft or the knowledge required to develop new chip designs cannot be contained in a crate. Such ideas do not stay within borders or include packing slips, and they are not subject to the scrutiny of customs inspectors. Once out of the country, knowledge cannot easily be reclaimed, repatriated, or destroyed. Controls on such collaboration must use the forces of technological progress to build the right fences around the right technologies, creating effective international export control regimes while allowing the United States to retain full discretion to impose unilateral controls based on policy and principle.

> The current country-based system of controls is becoming increasingly difficult to sustain.

A new hierarchy of controls should be considered to meet the requirements of these differing degrees of economic integration and technology collaboration. During the Cold War, countries rather neatly divided into blocs, and export control decisions were and still are largely based on those divisions. In today's global marketplace, however, potential rivals are also actual markets, and terrorists and WMD proliferators operate within the borders of friends and allies as well as enemies. The current country-based system of controls is thus becoming increasingly difficult to sustain.

To maximize economic benefit and national security in such a complex global environment, a revamped control system could use a three-step approach based first on customers and then on countries and technologies. Such an approach would refine the current system first by segmenting customers by reliability, then by permitting greater technology cooperation in countries with stronger technology-control regimes. Given an assessment of customer reliability and the strength of the national export control system, the system would then determine the level of technology that could be exported in any particular case.

The key to customer-based controls is information. Known "trusted" customers should have the freest possible access to sensitive technologies. Known "suspect" customers should be denied those technologies. "Gray area" customers, who cannot be categorized as trusted or suspect, then become the focus of export control scrutiny. Given the dynamism of today's global economy, with new companies constantly being formed and existing companies often being acquired or going out of business, a significant share of the customers or partners for technology cooperation could easily fall into such a gray area.

The goal of the system must then be to reduce the number of such gray-area customers by gaining enough information to move them into the trusted or suspect categories. Because customers may change over time, any system of technology controls will require a mechanism to reevaluate them periodically.

The Bush administration's 2006 proposal for an updated China export control policy takes an important step in this direction with its Validated End-User (VEU) program. Under the VEU program, certain civilian customers in China will be authorized to receive specified items that currently require export licenses without such licenses. To qualify as a trusted customer, a potential user will have to meet a number of criteria, including having a record of using U.S.-origin items for civilian uses only and agreeing to on-site visits from U.S. government officials. Certain items that currently require individual licenses for export to China can then be exported to the validated users without such licenses. The "trusted customer" status

> A new system could put the emphasis on the customer first.

will be subject to periodic reevaluation to ensure that the beneficiary continues to meet the program's criteria. The Bush administration plans to introduce this approach to India and will review opportunities to expand it to customers in other countries as well.

With primary emphasis on the customer, the country of that consumer takes on a secondary importance. Leaving behind the "good" country versus "bad" country construct, customer-based technology controls should evaluate individual countries by the strength of their technology control systems. In other words, having a country-specific policy would be a hedge against gray-area customers. A greater degree of uncertainty about a potential customer would be more tolerable in countries with strong controls because the technology would be less likely to be diverted into the wrong hands. Recent U.S.-Indian collaboration provides an excellent example of this approach. Through the Next Steps in Strategic Partnership initiative and the U.S.-India High Technology Cooperation Group, Washington and New Delhi have taken a series of reciprocal steps to expand the scope of permitted trade in sensitive technologies. Since 2004, India has implemented measures that strengthen confidence that sensitive U.S. technologies are used in accordance with U.S. law, including the passage of a comprehensive export control law to combat proliferation. In response, the United States has been able to ease certain restrictions on U.S. exports to India and is considering additional measures, as appropriate.

The final uncertainties over potential technology collaboration would be resolved based on the technology involved. It stands to reason that some technologies are so sensitive that they should only be transferred to the most

trusted customers in countries with the most stringent controls. Other technologies permit some margin for uncertainty. The basis for such a hierarchy of technologies exists in the differentiation between military systems and dual-use items. For the latter, there are also differentiators between items controlled for multilateral reasons or on the basis of unilateral U.S. foreign policy, national security, or regional stability. Therefore, although all major producing countries may agree that the export of most sensitive computers should be controlled in a wide range of countries, the United States may decide for its own reasons that it should limit the export of certain less-sensitive items, such as fingerprinting equipment, to human rights violators.

> Governments cannot fall into the trap of asking technology controls to do too much.

Applying a customer-based method to technology collaboration would yield a more tailored approach to controls, creating a system that considered the type and complexity of technology collaboration involved. For instance, recognizing the great advances in computing technology, the Bush administration in 2003 raised the technology control level for exports of general-purpose microprocessors to civilian customers. This freed billions of dollars in U.S. exports from licensing requirements. The liberalization did not apply to exports to military users, however, protecting national security. Thus, within the same economy, civilian customers now enjoy broad access to the chips they need to make their commercial products while military end users are subject to restrictions.

For more complex interactions such as research and development and manufacturing, controls must allow companies to maximize opportunities while safeguarding national security. Each company could draw up a custom risk-mitigation plan for government consideration based on the customer, country, and technology framework. Such an approach could draw on lessons from existing mitigation thinking and experience as contained in private sector "noncompete" agreements, merger and acquisition antitrust mitigation plans, risk-mitigation plans linked to approval of sensitive foreign investments by the U.S. government's Committee on Foreign Investment in the United States, and intellectual property protection policies.

Within the larger security structure, controls should be targeted to accomplish specified goals, designed to minimize negative impacts on businesses, supported by efforts to ensure the broadest possible international adherence, and enforceable. Technology controls have a major role to play in turning the potentially conflicting goals of cross-national technology collaboration and national security into a mutually reinforcing system of global secure innova-

tion. Yet, given the complexity of today's global economy, no single policy or system can successfully stand on its own. Security measures should be seen as a series of layers, from diplomacy to law enforcement to stronger measures, in which controls are only one form of protection. Considering this comprehensive approach to economic and national security, governments cannot fall into the trap of asking technology controls to do too much. Technology controls are most effective when used as a means of identifying specific risks and providing one of many screens to mitigate those risks. With technology controls, governments know what is dangerous and can take multiple steps, from policy to controls to negotiation to enforcement, to keep these items out of the wrong hands.

From Ideas to Action

Conceptualizing reform is the easy part; implementing it is more difficult. Any road map to reform must involve three important constituencies: Congress, the executive branch, and the private sector. Each has an important and legitimate voice in technology controls, and all must unify around a common vision of the threat and the solution. Since the end of the Cold War and the onset of globalization, achieving and maintaining international consensus on technology controls has grown more difficult. A focused, customer-based system tailored to new threats and based on common interests could rebuild consensus within the United States and among the international community.

In a world that is not divided into allies and adversaries but in which even allies unwillingly harbor terrorists and front companies for proliferators, concentrating on the end user of a technology is the best way to focus on what really matters: the impact of a particular, potential technology collaboration on security. It is far easier to agree on the need to keep missile components from a North Korean front company operating elsewhere in Asia or from biological weapons fermenters from al Qaeda cells in Europe than it is to agree on overall policy toward a complex country and economy such as China. A technology-based system would not only be more targeted, it would likely be more comprehensively enforced and therefore more effective.

Such unity might eventually pave the way for new legislation to replace the Export Administration Act (EAA), which was first passed in 1969 to update the Export Control Act of 1949. Not only have security threats and the global economy changed dramatically since then, but the EAA has been in lapse more often than not since the end of the Cold War, leaving the system to be administered under the president's emergency authorities.

Now is the time to begin the process of defining a new system of technology controls that enjoys broad support among the executive branch, Congress,

and industry. This article is intended as a modest, early contribution to what should become a thorough debate. The technology control system will have to cope with more intricate and sensitive products, new market realities, geopolitical changes, and the rise of substate actors. Globalization will not wait, so neither should such a complex task. The time is now to drop preconceptions, open minds, and launch the process for developing controls that will meet the security needs and economic challenges of the twenty-first century.