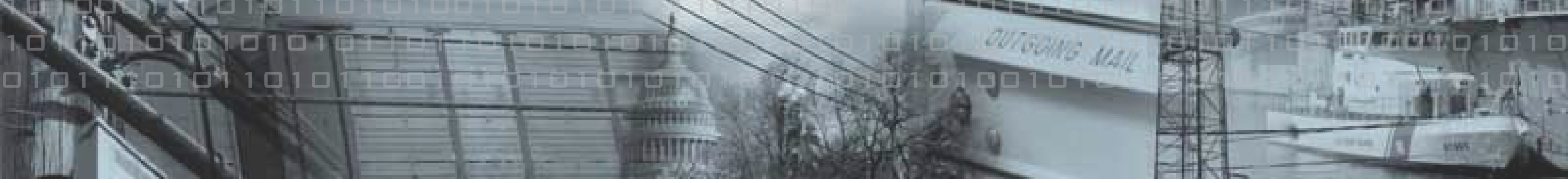

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

April 2014

Defense Industrial Base

Editorial Staff

Editor
Kendal Smith

Publisher
Melanie Gutmann

JMU Coordinators
Ben Delp
Ken Newbold

VOLUME 12 NUMBER 10

This month *The CIP Report* examines the **Defense Industrial Base (DIB)**. The DIB enables the research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, needed to meet US military requirements.[1]

First, Robert Mitchell of Temporal Defense Systems examines the potential implications for the DIB resulting from the National Telecommunications and Information Administration's decision to relinquish its oversight function of the Internet's Domain Names System. Dr. Terrence Guay next evaluates the DIB in light of impending budget cuts, changes in weapons systems, and global competition. TechAmerica's Scott Bousum and Rachel S. Wolkowitz then provide suggestions for collaborating to address cyber risk within defense supply chains. Finally, Dr. Harvey Sapolsky poses several questions for consideration as the DIB shrinks in response to reduced defense spending.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

[1]Department of Homeland Security, Defense Industrial Base Sector, available at http://www.dhs.gov/defense-industrial-base-sector.

The Loss of ICANN and Implications for the Defense Industrial Base

by Robert Mitchell, Co-Founder, Temporal Defense Systems*

On March 14, 2014, the US Department of Commerce's National Telecommunications and Information Administration (NTIA) announced its intent "to transition key Internet domain name functions to the global multi-stakeholder community."[1] Put simply, NTIA will give up its coordination and oversight function in the Internet's Domain Names System (DNS), effectively ending the US government's role as steward of the DNS and, more broadly, of the Internet itself. Functionally, the Internet Corporation for Assigned Names and Numbers (ICANN) handles this role under a contract with NTIA. That contract is due to expire on September 30, 2015. ICANN has been charged with developing a transition proposal prior to that date in collaboration with the multi-stakeholder community, consisting of the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Society (ISOC), the International Telecommunications Union (ITU), and the Regional Internet Registries (RIRs), among others.

Various authors have noted the potential harm to economic development and loss of Internet freedoms that may result from this decision. The focus has been on the likelihood of repressive governments limiting access or content and the resulting impact on human rights and free speech. While these are clearly important issues, the potential implications for US national security have yet to be examined, at least not publicly. With the rising tide of cyber attacks against US government agencies and strategic industries, the health of the Internet ecosystem must be a priority when considering national security and critical infrastructure protection objectives.

In broad terms, the ability of the United States to project force in support of national security requirements relies on worldwide communications and logistics. The US Defense Industrial Base (DIB), composed of "domestic and foreign entities and their subcontractors performing work for [the Department of Defense] (DOD) and other Federal departments and agencies,"[2] provides the foundation of this capability. By definition, "defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide."[3]

As a practical matter, the Internet provides the backbone for the vast majority of communications and logistics required to fulfill the aforementioned objectives through the contractual relationships that DOD makes with private sector firms that deliver required goods and services. The historical reliability and accessibility of the Internet is therefore a key component in both the health of the DIB and the US government's ability to project force. This statement may appear self-evident, but given the controversy over NTIA's announcement, it seems proper to consider the potential impact to the DIB.

What May Change

In the current ICANN governance model, functions such as security, interoperability, and contractual compliance fall under their purview. These functions are generally enforced through a series of agree-

(Continued on Page 3)

[1] Department of Commerce, National Telecommunications and Information Administration, "NTIA Announces Intent to Transition Key Internet Domain Name Functions," (Washington, DC: March 14, 2014), available at http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

[2] Department of Homeland Security and Department of Defense. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, (Washington, DC: Office of the Assistant Secretary of Defense, May 2007), at 5.

[3] Ibid.

(Continued from Page 2)

ments among the various parties involved in the operation of the Internet. In the transition to the multistakeholder ecosystem model, oversight of these agreements may pass to the United Nations' ITU. Critics of this approach argue that a "Balkanization" of the Internet would result, with individual nations such as China or Russia influencing the UN to limit Internet access or functionality among groups or individuals deemed undesirable.

The recent episode in Turkey, whose government banned access to Twitter and YouTube in response to leaked conversations among government officials, provides a glimpse of what may follow on a larger scale. In the case of Twitter and YouTube, there is an immediate and negative economic impact in losing access to such a large market. Imagine the impact if the ITU, influenced by US adversaries working through the UN, were to enact regional restrictions on Internet access to companies that support the DIB, especially during a time of conflict. What if certain categories of Internet traffic, such as encrypted communications, were subject to tariffs or sanctions? What if, in the midst of a crisis, a regional subsidiary of Lockheed or Raytheon lost the ability to communicate securely with US headquarters via virtual private network (VPN) or similar means?

The migration of functions to a more knowledge based transaction exacerbates this trend. For instance, DOD has researched the use of three dimensional (3D) printers to fabricate components in deployed locations. The advantages of this approach are obvious in reduced cost and logistical tail. However, the ability to transfer information electronically and collaborate in design and component revision requires free access to the Internet. Disruption in this communication medium could introduce complication in a process that is meant to solve logistical burdens.

In efforts to protect the DIB as a whole, how should the United States prepare for or respond to such scenarios? One possibility would be to create a parallel, standalone capability among designated DIB components to ensure reliable communications that do not rely on the open Internet. Satellite communications currently provide a means of secure voice and data transmission among military units worldwide, but are not suited to handle the necessary volume of traffic for commercial operations. Perhaps it is in the US strategic interest to invest in a similar system to address this potential vulnerability. That leaves open the question of who would bear the cost.

The NTIA decision on ICANN will take time to play out and the eventual outcome is not yet known. Nevertheless, in light of the possible negative impacts to the DIB if the Internet does not remain open and free, there is a clear need for the US government to establish specific interests and minimum terms with respect to any future changes in governing the Internet. Given the potential downside in ceding oversight, the cost of doing nothing may prove prohibitive.❖

** Robert Mitchell is Co-Founder of Temporal Defense Systems, a Seattle-based cyber security company. As a former Navy SEAL and CIA Paramilitary Officer, Mr. Mitchell has over 15 years of operational experience around the globe and regularly consults with US government agencies.*

The Defense Industrial Base in an Age of Uncertainty

by Terrence R. Guay, Ph.D., Smeal College of Business,
The Pennsylvania State University*

The US defense industry dominates global armaments production, and has done so for decades. In all likelihood, its international influence will continue going forward. But there are three important factors that will shape company production, staffing, and strategy decisions over the next decade: impending cuts to the US defense budget; the continued shift away from traditional weapons systems; and increased competition in the global armaments market.

Table 1 lists the top ten US companies based on 2012 global defense revenues. The industry is dominated by five companies: Lockheed Martin; Boeing, Raytheon; General Dynamics; and Northrop Grumman. Together, they combined for more than $140 billion in defense revenues in 2012. However, the US defense industrial base also consists of foreign companies with extensive US operations. United Kingdom-based BAE Systems, for example, employs approximately 43,000 workers in the United States, and roughly 40 percent of the company's global sales are to the Pentagon. Given the overlap between the defense industry with other sectors (particularly aerospace and electronics), precise employment figures are difficult to discern, but several studies place the number at a little more than one million workers in the private sector. A 2012 report by Deloitte calculated that the economic impact of the defense industry generates an additional 845,000 federal government jobs, and 2.5 million indirect jobs.[1]

It is helpful to place the position of the US defense industrial base in historical perspective. The defense build-up that began in the late 1970s and continued for more than a decade resulted in the growth of many large companies. However, with the end of the Cold War, there was significant over-capacity in the defense sector. Declines in the US defense budget, as well as arms-importing

(Continued on Page 5)

Company	2012 Defense Revenues (billions)	2012 Total Revenues (billions)	Defense Revenues as Percentage of Total
Lockheed Martin	$44,883	47,182	95.1%
Boeing	31,378	81,698	38.4
Raytheon	22,705	24,414	93.0
General Dynamics	21,023	31,513	66.7
Northrop Grumman	20,600	25,218	81.7
United Technologies	12,117	57,700	21.0
L-3 Communications	10,839	13,146	82.5
SAIC	8,301	11,200	74.1
Huntington Ingalls Industries	6,240	6,710	93.0
Honeywell	5,100	37,700	13.5

Table 1: Largest US Defense Companies[2]

[1] Deloitte, *The Aerospace and Defense Industry in the U.S.: A Financial and Economic Impact Study*, March 2012, http://www.aia-aerospace.org/assets/deloitte_study_2012.pdf.

[2] Source: *Defense News,* Top 100 for 2013, http://special.defensenews.com/top-100/charts/rank_2013.php.

(Continued from Page 4)

allies in Europe, led to an industry consolidation through mergers and acquisitions. The defense sector was transformed yet again after the September 11, 2001 terrorist attacks. Military leaders began to prioritize command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) over more traditional weapons systems like aircraft, ships, and tanks—an orientation that continues to the present day.

Yet, the future dominance of this sector will be shaped by three inter-connected factors over the next decade. The first is budgetary. It has become clear in recent years that the key actors in Washington, including both political parties and the executive and legislative branches, are aiming to move toward a more balanced budget. Although the mix of spending cuts and tax increases is subject to the political winds, it is quite clear that, short of a major international conflict that directly impacts US national security, the defense budget—particularly weapons procurement—will be sharply cut. The Budget Control Act of 2011 imposes spending caps, effectively keeping the Pentagon's base budget flat over the next decade, but it is entirely possible that further cuts will be made over the coming years. The implications for defense companies are to diversify their markets, mainly by obtaining more non-defense business. Indeed, that is the strategy pursued by some of the largest companies. In 2005, Boeing derived 56 percent of its revenue from defense. By 2012, it had dropped to 38 percent. Similar, although less dramatic, declines were experienced by Lockheed Martin (98 percent to 95 percent), General Dynamics (78 percent to 67 percent), and L-3 Communications (91 percent to 83 percent)—even as total revenues grew. However, some companies have intensified their efforts by providing a wider array of weapons systems to take advantage of the opportunities provided by the spending peaks in recent years. Raytheon increased its reliance on the defense sector from 83 percent of total sales in 2005 to 93 percent in 2012, while Northrop Grumman increased its exposure from 76 percent to 82 percent, even after spinning off its shipbuilding business in 2011 to create Huntington Ingalls Industries. These latter companies are likely to be most affected by the impending defense budget cuts.

The second factor that will shape the evolution of the US defense sector in the short to medium-term is the continuing trend toward increasing use of C4ISR. As the military focuses more resources on the high-technology dimensions of security—particularly areas like intelligence, surveillance, and reconnaissance—companies who specialize in these areas are moving up the rankings, and firms with expertise in more traditional military hardware (e.g., planes, ships, tanks, and armored vehicles) are expanding their operations into these other products and technologies. This explains part of the increased reliance on defense revenues described above. For example, SAIC was the 12th largest US defense contractor in 2000 (based on 1998 defense revenues), but now ranks 8th, according to *Defense News*. L-3 Communications moved from 22nd to 7th over the same time period. With the declining need for military hardware due to the drawdowns in Iraq and Afghanistan, the Pentagon is seeking to allocate scarce procurement dollars to maintaining a technological edge over potential adversaries. Thus, the proposed 2015 defense budget aims to eliminate programs like the A-10 aircraft, but spend more on the Global Hawk reconnaissance drone and cyber security.

The third factor relates to the global environment and the opportunities for arms sales. Exports long have been important for the US defense industry. However, the impact of US defense budget cuts in the near-term makes global sales imperative. Between 2004 and 2012, international sales at Boeing's defense division increased from 7 percent of the company's defense revenue to 24 percent.[3] For Raytheon, foreign sales grew from 16 percent to 26 percent. The global market for weapons is undergoing important changes. European governments slashed defense spending starting in the early years after the Cold War, and more recently due to the region's economic crisis and use of austerity measures by some governments

(Continued on Page 6)

[3] David Lerman and Robert Wall, "U.S. Defense Contractors Focus on Foreign Buyers," *Business Week*, November 14, 2013, http://www.businessweek.com/articles/2013-11-14/2014-outlook-u-dot-s-dot-defense-contractors-focus-on-foreign-buyers.

(Continued from Page 5)

to improve their countries' deficit and debt levels. Since US defense spending comprises about 40 percent of the global total, cuts in the US will have a disproportionate effect on international arms sales. This means competition for arms sales in markets outside the NATO region will intensify.

Table 2 reflects the increased competition over the two most recent five year periods. The market share of US defense companies declined slightly by 1 percent, while the share of the top five European producers (Germany, France, United Kingdom, Spain, and Italy) dropped from a combined 27 percent in 2004-2008 to 22 percent over 2009-2013. The implication is that competition from firms domiciled in Russia, China, and other countries will place greater pressure on US defense companies for sales in growing markets like Asia (where imports grew by 34 percent over these periods) and Africa (53 percent), and certain countries like Brazil (65 percent).

The increased level of competition mirrors the changes that non-defense companies have experienced in international business for over a decade. While Russia long has been a major player in the global arms trade, China has not. US defense companies should expect more competition from Chinese and other emerging market defense companies in the coming years, although these firms' cost advantages will not be as effective an entry strategy when technological sophistication and foreign policy considerations will continue to favor the US industry.

To summarize, the US defense industry is facing what has become a once-per-decade adjustment to product development, operation considerations, and global strategy. Budgetary pressures, a reorientation in military strategy and the weapons required to fulfill it, and increased global competition have converged to create a period of uncertainty, but also of opportunity. Given the relatively few mergers and acquisitions in this sector over the past 15 years, the time may be ripe for a new round of industry consolidation as larger firms that have gradually shifted parts of their revenues to the non-defense sector hedge their bets by acquiring C4ISR companies that are closely wedded to the Pentagon's more recent acquisition focus. While such actions would require the blessings of the federal government, there is reason to believe that they would be bestowed since it would allow the preservation of key components of the US defense industrial base and continued relationships with well-established corporate names.❖

**Terrence R. Guay is Clinical Professor of International Business at the Smeal College of Business at The Pennsylvania State University, where he teaches undergraduate and MBA international business courses. His research focuses on the competition between governments, international organizations, NGOs, and other non-state actors to shape business behavior and the global business environment. He has published three books and monographs and numerous journal articles and book chapters on defense industry-related issues.*

	2004-2008	2009-2013
United States	30%	29%
Russia	24	27
Germany	10	7
China	2	6
France	9	5
United Kingdom	4	4
Spain	2	3
Ukraine	2	3
Italy	2	3
Israel	2	2
Others	13	11

Table 2: Share of World's Arms Exports[4]

[4] Source: Siemon T. Wezeman and Pieter D. Wezeman,"Trends in International Arms Transfers, 2013," Stockholm International Peace Research Institute, 2014, http://books.sipri.org/files/FS/SIPRIFS1403.pdf

Sharing Accountability to Create a Cybersecurity Risk Framework

by Scott Bousum and Rachel S. Wolkowitz*

Background

On February 12, 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636). Taking the first step towards implementing the EO, the General Services Administration (GSA) and the Department of Defense (DOD) submitted joint recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration, and addressing what steps can be taken to harmonize existing procurement requirements related to cybersecurity. Specifically, they made six recommendations:

1. institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions;

2. address cybersecurity in relevant training;

3. develop common cybersecurity definitions for federal acquisitions;

4. institute a federal acquisition cyber risk management strategy;

5. include a requirement to purchase from original equipment or component manufacturers, their authorized resellers, or other trusted sources for appropriate acquisitions; and

6. increase government accountability for cyber risk management.[1]

Many Players; One Goal

To put the joint recommendations in context, though we talk about a "technology industry" and Silicon Valley as if the information and communications technology sector is a monolith based in one area, reality betrays much more nuance and variation than the same implies. For example, hardware is represented by manufacturer hardware products, resellers and distributors, wholesalers, brokers who are suppliers of those hardware products, and integrators that develop intricate weapons platforms and information systems using those hardware products. Steps to mitigate or eliminate cyber threats in the manufacturing phase would provide little protection for integrations. Requirements for hardware almost certainly do not address critical risks that present themselves in software.

Hierarchy of Criticality

To successfully address cyber risk, government and industry must identify a hierarchy of critical attributes on a program-by-program basis as minimal supply chain assurance criteria. Any additional mission or program-critical criteria should be recognized as part of the requirements for an acquisition and should be approached as a separate measure to a secure supply chain. A tiered structure would allow industry to provide a measure of protection against counterfeits or malicious code and avoid government-unique requirements. Government-unique requirements should only be included in high-risk contracts.

Different Players; Different Needs

As TechAmerica identified these areas of interest, it resulted in our ability to ask our member companies in each community within the technology sector to assess specific needs and to categorize possibilities for consideration as metrics to assess cyber assurance. The endorsements we garnered, broken out by sector, follow.

Hardware Integrators have a history of addressing these issues because many of the products they incorporate fall into the sixteen critical infrastructure sectors described in

(Continued on Page 8)

[1] Department of Defense and General Services Administration. *Improving Cybersecurity and Resilience through Acquisition*, (Washington, DC, Office of Secretary of Defense, November 2013), at 7-8.

(Continued from Page 7)

the risk-based hierarchy. Similarly, their customers have a record of identifying those elements of a program or contract that require additional protections. As a baseline requirement, hardware integrators would recommend the government look to best practices or standards that adequately measure efforts to protect against cyber threats in a reasonably managed fashion. These consensus based standards are recognized in the integrator community and have been adopted by Federal Agencies as a requirement for their acquisition purposes.

Software integration is distinct from hardware development because it can range from the writing of whole programs to making minor modifications to the firmware operating a hardware product. The government should consider the effects and potential costs of holding software integrators to the same assurance standards that software developers are held.

Original Equipment Manufacturers have also focused on securing their supply chains because controlling quality is a critical element of brand integrity. Most of the companies competing for government work or supplying integrators often have a more robust commercial market presence, and for all of them, whether in both markets or focused entirely on the public sector, ensuring product integrity includes keeping cyber threats out of the supply chain.

When the government selects a supplier or software vendor, a range of factors are relevant to the decision making process, including the product's ability to perform as required and the quality of the engineering practices that went into designing, building, and delivering it to the government. Therefore, the efforts understandably revolve around how to ensure that the security of trustworthy products, including software, is not compromised by virtue of genuine articles being swapped out for counterfeit ones that could pose a cyber-threat.

To better understand the steps software developers take to promote security, it would be worthwhile to look at best practices for the development of genuine software within the industry and how such efforts contribute to government supply chain security. For example, Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain, a report issued by the Software Assurance Forum for Excellence in Code, or SAFECode, provides best practices for secure software development for a software engineering and development audience. SAFECode also released a follow-on report, Fundamental Practices for Secure Software Development. Other options that the Working Group should examine are the Information Technology Infrastructure Library (ITIL), or the (ISC)2 Organization's Certified Secure Software Lifecycle Professional (CSSLP). Both frameworks offer guidance on software development that can provide a measurement of software supply chain assurance for genuine products.

Services Providers, including cloud and data center services, are companies who sell capabilities based on hardware and software provided over the Internet in a public or private network. TechAmerica members propose decision makers consider that the Federal Risk and Authorization Management Program (FedRAMP) process—supported government-wide—incorporate specific controls that require the demonstration of supply chain assurance equal to any demonstration required for hardware, software, or services delivered directly to the government. In other words, if a server or router was acquired as part of a cloud or data center service, then FedRAMP would have to include supply chain assurance demonstrations that the same server or router would have to make if it were being delivered directly to the government. This recommendation would address all communities on our grid that are identified as OEMs, resellers, distributors, wholesalers and brokers, and integrators for all information technology services.

The last set of communities identified on our grid of the tech sector are those companies reselling goods and services, but who are neither the manufacturers or developers of those goods or services nor the integrators of those goods or services. This community frequently offers products to the government that the original equipment manufacturer chooses not to offer directly. A concentration of these vendors selling hardware, software, and services is on the Schedule contracts managed by GSA.

(Continued on Page 9)

(Continued from Page 8)

Knowing Your Seller

Resellers, distributors, wholesalers, and others who have an authorized relationship with the original software developer or hardware manufacturer present the lowest risk for the supply chain. When possible, products should be purchased directly from the original manufacturer or its authorized distributor, or through suppliers that furnish products acquired directly from the original manufacturer or its authorized distributors. Chain of custody documentation should be inspected as part of government acceptance to ensure that products have not been tampered with. Regulations and policies must allow for the exclusion of independent distributors and brokers when products are available from the OEM or an authorized supplier. In the software and cloud spaces, the government must be wary of phishing sites and others that aim to mimic the look and feel of genuine software and services.

TechAmerica acknowledges that moving to an authorization requirement for vending hardware, software, or services to the government proves a challenge for some companies, particularly the multitude found on the GSA Schedules. Many in this multitude are small businesses, and this conflict between a reasonable means to eliminate counterfeit items from the government supply chain and lower barriers for business entry into the public sector market is another of the disconnects in current policy we noted earlier. To alleviate any hardship such a requirement may impose, the government should create an incentive program for those companies. Possible incentives include the ability to remain on the Schedules or other government contracts, and additional monetary incentives that can offset the impact such a restriction may have.

Conclusions

As software and cloud services take on increased roles in government services and acquisition, cybersecurity must take a more prominent role in securing the supply chain and our critical infrastructure. The government has taken the first step towards recognizing the threat and developing recommendations in acquisition that demand the joint participation of industry and government agencies. More specifically, the "industry" component must be broken-down further to ensure the most effective and appropriate actions are taken to address cyber risk.❖

** Scott Bousum serves as the Director of National Security Policy, Global Public Sector for TechAmerica, the leading US technology trade association.*

Rachel S. Wolkowitz serves as the Assistant General Counsel for TechAmerica, the leading US technology trade association.

Questions to Ask as we Shrink the Defense Industrial Base

by Harvey M. Sapolsky, Ph.D.*

Defense spending in the United States seems certain to continue its decline after the troop withdrawals from Iraq and Afghanistan are completed. The defense budget doubled after the 9/11 attacks against America's homeland.[1] With both Osama bin Laden and Saddam Husain dead, and the record established that groups or states targeting Americans will pay a terrible price, it appears likely that defense spending will soon be affected by factors that pull in the opposite direction of the budget boosting 9/11 attacks.

None of these factors—potential challenges by peer competitors, changes in warfare, and the demand of other governmental obligations—will stop the decline in the size of the American defense industrial base, which tracks the defense budget. Russia and China pose only a shadow of the threat posed by the now long defunct Soviet Union. Warfare has become a precision exercise, shrinking the need for the mass production of weapon systems and making mass formations of forces obsolete. And the demands of government spending on health care for an aging population alone will surely squeeze the rest of government, defense spending included.

Yet there is no zero option for defense. The American military will fight again in wars that can only be dimly imagined today and in totally unexpected places. We are usually surprised and unprepared for our wars. We weren't ready for World War I and II, and were caught short by Korea, Vietnam, and the Global War on Terror. There is, though, a floor to defense spending built around America's global role that was assured by World War II's outcome, the professionalism that came with the long mobilization for the Cold War, and the set of political and organizational interests that have come to live off the defense budget—the armed services, communities near military bases, our free-riding allies, and, yes, the defense industry. Something fairly substantial will be left in defense.

The defense industry dependency is intertwined with that of the government. Prior to World War II, America prepared for war in the long periods of peace by maintaining a set of government owned and run arsenals and shipyards where new weapon designs were developed and produced in the small quantities needed to supply our small peacetime military. There was not enough of a domestic business to sustain much of a private arms industry. When war arrived, contractors were hired to produce on a mass scale. Aviation became an early exception because aviation technology progress was so rapid that contracting became the inter-war norm. With the Cold War mobilization, weapon design, development, and production in all weapons areas shifted almost entirely to contractors. The peacetime dollars government spent on defense were big enough to sustain contractors, and the technological change in weapons was too fast for the arsenals to keep up. The surviving arsenals and shipyards concentrated on repair and overhaul activities. Contractors became our private arsenals, as dependent upon the government for their profits as the government was dependent upon the privately held contractors for its weapons in both peace and war.

The test of this system comes now as peace appears to be returning—we hope this time for longer than the decade of peace that fell between the end of the Cold War and 9/11 attacks. The Army is slated to decrease by 100,000 soldiers, while the other services may lose almost as many combined.[2] With the cost of personnel increased due to enhanced salaries and benefits

(Continued on Page 11)

[1] Adm. Gary Roughead and Kori Schake. *National Defense in a Time of Change*. Washington, DC: The Hamilton Project, February 2013, at 7, available at: http://www.ngaus.org/sites/default/files/HamiltonProjectBrookingsRougheadPaper2013.pdf.

[2] Tom Vanden Brook, "Budget Plan would Slash Army by 100,000 Soldiers," *USA Today*, January 18, 2014, available at: http://www.usatoday.com/story/news/nation/2014/01/18/army-budget-cuts-national-guard-sequestration/4635369/.

(Continued from Page 10)

approved during the Global War on Terror, funds available for procurement are likely to drop by as much as half. Lobbying will slow the erosion, but not the need for industrial triage.

What to save? The first priority should be defense research and development activities. America has a substantial military technological edge over others. It is the way we prefer to fight. Our defense budget is 42-45 percent of global defense expenditures, but we account for over 80 percent of global defense R&D. We need to have the best UAVs, robots, satellites, and sensors. The portfolio of projects should be broad and deep as we cannot predict in which types of warfare and geographic areas future challenges will develop. Our network of defense research facilities—public and private laboratories—needs to be well supported.

What to produce? We have plenty of first line aircraft, armored vehicles, and ships in our inventory. What we need are more prototypes of new systems and experimental units to test new designs and concepts. The experiments should be realistic so as to provide guidance on what might be produced in larger numbers when threats become clear and action is imminent.

What subsectors need special attention? The United States has the largest economy in the world and is capable of producing nearly everything it needs. It is dominant in commercial aviation, and thus could produce military aircraft easily even if military production halted entirely. The same is true in commercial electronics, heavy vehicles, and dozens of others fields of military relevance. There are some important exceptions, however. Submarines have no commercial analogs; so too for nuclear weapons. For these subsectors and a few others, the government must support production facilities and skills as well as a design capability. It is an industrial insurance policy that may be necessary for decades.

But there is a danger in saving too much. Military technology is dynamic. Casualty concerns will change the role of soldiers on the battlefield and require new methods for defeating opponents. We will learn to fight wars differently and look for new ways to deter them. Despite Secretary Rumsfeld's response to complaints of unpreparedness with the assertion that you fight wars with the army you have,[3] we do in fact mobilize for wars, cranking up and redesigning the machine that is mostly on standby mode to influence the outcome of wars as we fight them. We seek to adapt to the contest at hand. Resources devoted to preserving past capabilities can hurt our ability to meet the defense needs of the future. We must choose wisely.❖

* *Harvey M. Sapolsky is Professor of Public Policy and Organization, Emeritus, at the Massachusetts Institute of Technology and the former director of the MIT Security Studies Program.*

[3] US Secretary of Defense Donald Rumsfeld, Town Hall Meeting in Kuwait, December 8, 2004, available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=1980.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1