ASA

Risk Consultants

Research Note

Risk Themes for America's Defense Industrial Base Sector

By: Casey Rodgers

Keywords: Defense Industrial Base, Military Industrial Complex, Intellectual Property, Defense Contracting, Risk Management, National Security, Homeland Defense

Abstract: The Defense Industrial Base sector is a key source of American national security technology and a major driver of the American economy. The sector faces a multitude of risks across a variety of categorical groupings. This research note outlines three major categorical risk themes with an adjoining risk assessment of a specific risk source followed by treatment suggestions for each category. Topics such as intellectual property theft, contractor safety and economic espionage with a focus towards increasing public-private sector coordination in the Defense Industrial Base sector are also examined.

Introduction

The Defense Industrial Base (DIB) sector describes the global industrial complex that supplies the world's governments and militaries with defense technologies, research, support, logistics and many other vital services.[1] The DIB sector is an enormously important American asset, not only for national security and defense but also as a powerful economic engine. The sector is truly worldwide with over 100,000 component companies and contractors employing millions of highly skilled technical and mechanical workers.[2] The sector's integral position in the United States' national security and economic strategy makes the sector an enticing target for other companies, militaries, terrorists and foreign governments.

The DIB has to manage a myriad of risks within a highly competitive business environment while meeting the contractual and legal obligations stipulated by their patrons. This research note will begin with a brief description of the current risk management framework being employed by the sector including a description of the structure, participants and stakeholder needs. After which, a broad risk identification process will be discussed, while singling out key risks for

more detailed assessment, including historical anecdotes and terminating with treatment suggestions for each categorical risk source.

Sector Description

The many U.S. Critical Infrastructure and Key Resource (CIKR) sectors are managed under a very large bureaucratic umbrella that incorporates both public and private sector partners. The current bureaucratic framework and its executive backing is buttressed by the Homeland Security Presidential Directive-7 (HSPD-7), written by the Bush Administration in 2003.[3] The directive replaced President Bill Clinton's earlier directives with expanded attention given to the prevention and response to acts of terrorism that would affect the U.S. critical infrastructure. The directive forges a coherent national policy for the identification and protection of the systems that permit and maintain basic functioning of the U.S. economy and society. Additionally, the HSPD-7 seeks to limit the impact of attacks on key resources and build cooperative systems between all the levels of government and private industry working within critical infrastructure sectors.[4]

The strategic imperatives of HSPD-7 are tactically addressed in the National Infrastructure Protection Plan (NIPP) which contains a sector-

specific plan for the Defense Industrial Base sector. The Department of Defense (DOD) serves as the Sector-Specific Agency (SSA) charged with building, managing and updating the DIB's portion of the NIPP and works closely with other related executive branch agencies to manage the sector.

These agencies make up the Government Coordinating Council (GCC) which collaborates with its private counterpart the Sector Coordinating Council (SCC). The SCC is made up of private industry owners and operators in the DIB eco-system and the two councils share a forum as the Critical Infrastructure Partnership Advisory Council among other bureaucratic relationships and acronyms. Together the councils have worked to implement an "all-hazards" risk management approach with goals to improve information sharing, cyber-security and sector resilience.[5]

Risk Themes, Key Issues and Treatment Recommendations

The following sections identify the broader risk themes and the challenges that they pose to the sector's growth, security and economic viability. The broader themes will be treated as categorical supersets of similar risk sources and exposures. The purpose is to illustrate the sheer

number of risks, the strategic goals they imperil and to offer anecdotal evidence on threats and vulnerabilities. Within each risk category a single risk issue is highlighted for a more detailed qualitative assessment and offer broad treatment recommendations for each category.

Risks to Competitive Advantage

This category contains risks that impact the DIB sector's ability to not only meet mission-critical security goals, but also risks to the sector's ability to meaningfully contribute to U.S. economic prosperity and stability. The private companies comprising the Defense Industrial Base sector are some of the most successful and unique organizations in the modern U.S. economy. The top five U.S. based defense contracting firms are all ranked within the Fortune 100, and combined these companies generated over a quarter-trillion USD in revenue last year.[6] The defense industry and the larger Military Industrial Complex is a major employer of skilled labor, scientists and engineers. Again, the top five defense firms employ over 730,000 workers, many of which provide skilled mechanical and scientific labor.[7] These workers are a national resource in dwindling supply and they meaningfully contribute

to the nation's security and economy through their relative rarity and unique skill sets.

The single highest risk source in this category is Intellectual Property (IP) theft. The organized theft of defense industry IP erodes the sector's ability to compete for contracts and deters investment in expensive capitol research and development projects. The exfiltration and illegal utilization of intellectual property is performed by many different actors in pursuit of varied end goals. The competitive advantage of the U.S. DIB sector is attacked through traditional, industrial and economic espionage carried out by both friendly and adversarial nation states as well as other firms. The IP shakedown is performed in multitudinous ways ranging from cyber-intrusion, to simple bribes and breeches in physical security, to foreign intelligence agency penetration, and so on.[8]

The sector itself is a competitive high-stakes market space and there have been numerous cases of industrial espionage carried out by defense contracting firms against inter-sector competitors in pursuit of high-dollar government projects. For example, in 1998 the Boeing Company was successfully awarded a number of lucrative launch vehicle contracts over its chief competitor Lockheed Martin, only to

have them revoked when officials realized that Boeing had procured confidential bidding documents from insiders within Lockheed Martin. The espionage effort resulted in considerable Justice Department scrutiny and later snowballed into a massive $615 million settlement between Boeing and the federal government.[9] Additionally, foreign intelligence agencies routinely attempt to penetrate the DIB sector through employment and human intelligence assets in an effort to steal intellectual property and gain insight into U.S. military strategies and systems.

Examining the risk category at large we see that there exists enormous loss potential in dollars, security and innovation. The loss potential combined with the many different attackers clearly demonstrating both the capability; as well the intent to target the DIB sector's competitive advantage brings the risk profile into better view.

Key Risk – State Sponsored Economic Espionage

The defense industry is a potentially rich source of economic intelligence for a foreign nation state actor. The enormous costs associated with doing groundbreaking research and development is a major barrier for countries looking to modernize their economic and military strength. Put frankly, it is generally cheaper to simply steal

someone else's research than to attempt to develop the knowledge organically. The scale and overall cost of economic espionage to the United States economy is shocking. Exact figures are difficult to produce but a recent report undertaken by the Commission on the Theft of American Intellectual Property states that annual impact to the U.S. economy exceeds $300 billion.[10] To put this amount in perspective, the annual losses of IP to theft and espionage at least equal the value of all U.S. exports to Asia.[11] If similar legal standards were applied to IP theft abroad like the ones used here in the U.S. it would translate to millions of American jobs.[12]

The IP commission generally agrees with a quote made by NSA Director General Keith Alexander that the current levels of Intellectual Property theft amount to "the greatest transfer of wealth in history."[13] That said, when assessing our nation's and the DIB sector's risk exposure we can state that both the significance and the likelihood are high that a current economic espionage threat is exploiting the many vulnerable aspects of the Defense Industrial Base sector. Complicating the problem further is the rapid development of IP theft methodologies that now include the use of sophisticated malware, cyber-intrusion for the purpose of data exfiltration and even the infiltration of companies

by intelligence agents.[14] In essence, not only the Defense Industrial Base sector but the outright viability of the American economy and national security apparatus is being eroded year over year with little hope for cessation without major changes that span the public and private sector divide.

Treatment Recommendations

The situation is relatively dire yet there are some steps that can be taken in the short term to hopefully work towards managing our nation's key resource risks. Firstly, strengthen supply chain oversight and accountability to allow for the speedier and more accurate identification of Intellectual Property loss and make possible the tracking of goods that were manufactured using stolen intellectual property.

Second, allow provisions for the Treasury Department to sanction and exclude companies engaging in IP theft from participation in the United States banking and financial markets. This would provide some consequences in the short term for proven offenders and hopefully help to deter future thefts.[15] Finally, address the human intellectual capital issues that arise from educating foreign students in American university system and not granting them the immigration status to

work, reside, or eventually gain citizenship in the United States. Our higher education system is a source and focal dissemination point of valuable IP and if we do not provide foreign students the opportunity to work here then they will take those skills to competing companies abroad.[16]

Physical Risk Theme

Defense Industrial Base partners have to consider the risks to the physical safety and personal wellbeing of people as well as their electronic devices, paper documents and other media when traveling and working abroad. Of paramount consideration is the historical precedent of targeting contractors for kidnapping, detainment, or even outright violence. The defense industry must travel to serve its distributed client base and often must move through or operate within active conflict zones or locations where the rule of law has effectively broken down.

The sector has a moral and pragmatic mandate to provide adequate protection to its employees when required to work in areas where physical violence or martial conflict is common. Sector members must also analyze and treat the risks endemic to electronic devices that handle, store or transmit sensitive material like design drawings,

financial figures or strategic company goals. The amount of proprietary information capable of being stored on your average Blackberry is really quite incredible let alone the quantities routinely handled by external storage devices, laptops, or tablet computers. These devices present a significant source of potential risk exposure when not properly configured, secured or operated. Contractors moving through high-traffic areas where people and items are scrutinized can expose valuable trade secrets to foreign intelligence actors and industry competitors if preventative measures are not employed. There are innumerable anecdotes that show the relative danger to devices and documents when simply transiting an airport or mass transportation facility. Abundant stores of personally identifiable information or other meaningful data are lost by unwitting travelers that lose bags or have their luggage stolen while traveling. Failure to implement basic information security risk mitigation steps like full disk encryption, device locking and password complexity can leave vital information highly vulnerable to interception.

Key Risk – Personnel Security in Warzones

Sadly, contractors are a “soft-target” when they have to work in warzones or conflict areas. Attacking American contractors offers

terrorists the same opportunity to inflict psychic harm as attacking U.S. soldiers without many of the mortal risks. Participation in the defense industry is often interpreted by extremists as open support for the oppression of occupied peoples and thus terrorists have and will likely continue to kill, kidnap and maim foreign contractors. The images from the 2004 Fallujah ambush of four American private military contractors are still fresh in the minds of many, and show that there are losses greater than dollars or nebulous abstractions like competitive advantage and intellectual property.[17]

Assessment for this is simple. There is no higher impact than the loss of human life and thus the significance rating is being given the label “extreme” to denote its potential effect on life and limb. The likelihood determination is more difficult. We can assume that the overall percentage of contractors that are attacked while working abroad is quite low but it does happen in nearly every major armed conflict. Despite a lower probability, the potential significance is so costly that the risk exposure rating for personnel in warzones is still high.

Treatment Recommendations

To counteract threats to personnel working abroad there needs to be an effort to increase information sharing, threat intelligence, training and collaboration between the Pentagon and contractors operating in areas where the U.S. military is active. The DIB sector should create a best practices plan to outline the preparations and security precautions that companies must provide when sending employees into dangerous areas. The plan could emphasize the baseline level of security required to show that companies and public agencies are very seriously considering the risk exposures endured by foreign deployed workers. The sector must go where they are required in pursuit of national defense and military support, but those travels must be made in a way that protects human life above all else. The sector can achieve greater alignment through collaborative threat sharing and analysis that will seek to determine when the risk exposure to non-military personnel is inordinately high.

Functional Risk Themes

The functional risk category contains risks that imperil the Defense Industrial Base sector's ability to function in a desired or acceptable state. This umbrella group of potential risk exposures

imperils the sector's ability to deliver down-stream goods with the requisite level of quality in a timely and compliant fashion. Our modern global economy has created new modes of production and collaboration that are presently stretching the sector's ability to meet the contractual demands of its clientele. The degree to which the defense industrial base relies on sub-contractors and other producers of component parts is quite astonishing and makes quality assurance, regulatory compliance and vendor management extremely difficult.

Currently, the lack of oversight and standardization within the defense industry's global supply chain creates conditions in which the integrity of the production process is called into question. There is no agreed upon standard or even a best practices guide for insuring accountability and traceability within the supply chain and thus each link in the chain assumes that their sub-contractors are performing their due diligence. The lack of cohesion and auditability of the entire end-to-end system creates risk exposure that is inherently difficult to treat since its causation and attribution is distributed across a number of regulatory areas and geographical regions.

The Defense Industrial Base faces future hardships with the prospect of lowered military expenditures, budget cuts and the looming

prospect of sequestration.[18] The sector has profited immensely during the long period of uninterrupted military expenditure growth that came with the Cold War and extended through the War on Terror, but things are likely to change after a decade of continuous warfare.

During the years of elevated military spending the private sector companies have become over-reliant on the U.S. Federal Government and Department of Defense for contracts. Of great concern is the relative lack of commercial applicability that much of the defense sector's products have. As much as any private citizen would like to be the owner of a brand new M1A1 Abrams Tank, most consumers can't swing the $4,350,000 sticker price and thus in the face of sequester the industry needs to retool its offerings to have broader market appeal.[19] In order for the DIB sector to continue innovation efforts and costly research and development initiatives the sector must have a stable revenue stream, else it is likely we might see a degradation in capability and future unwillingness to take on expensive capital investment projects.

Key Risk – Extended Supply Chains and Counterfeit Components

The intricacies of the military industrial complex make supply chain management, monitoring and security extremely difficult. The

number of component systems and technologies required to design, build and maintain a modern weapons system is huge. The fidelity and integrity of U.S. military technology is jeopardized when supply chains become unwieldy and over-extended.[20]

Enormous supply chains are vulnerable to the insertion of counterfeit goods that are made using stolen intellectual property and manufactured in facilities that do not engage in proper quality assurance strategies. The threat here is that the unnoticed supply chain absorption of counterfeit components might cause critical systems to fail or be vulnerable to compromise. There is already evidence that the defense industry's supply chain has lost integrity.[21] A 2010 study funded by the Naval Air Systems Command found that nearly 40% of survey respondents reported finding counterfeit electronics within their supply chain at all levels.[22] Worse yet, the study displays the near total lack of standardization for record keeping, auditing and traceability within the industry and supply chain.[23]

Assessing DIB sector risk exposure here is inherently difficult. The global supply chain is sufficiently lacking in transparency and reporting mechanisms. The significance of vulnerable supply chain management procedures being exploited by unscrupulous or even outright malicious

sub-contractors is potentially enormous but it likely ranges widely depending on the circumstances. Judging the earlier mentioned study, we can see that counterfeit items are routinely making it into the defense industry's supply chain at many different points.

Our risk exposure here is largely indeterminate without greater reporting data on the consequences that counterfeit items can have on complex military systems. Ultimately, the issues are going to require cooperation between the sector's private companies and their vendors to agree upon compliance standard and oversight controls. The public sector can offer assistance by drafting an enforceable legislative framework to empower any agreed upon standards.

Treatment Recommendations

Defense firms and especially the Pentagon, with its role as the most likely end consumer of defense products, must engage in a more rigorous and well documented testing procedure for parts as they move through the global supply chain. Performing testing will allow the sector to generate a list of trusted suppliers and isolate other suppliers that are failing to maintain a requisite level of quality assurance.

The sector needs to lean on legislators to mandate that upstream defense suppliers adopt a standardized system for recording the detection of counterfeit items that will provide traceability during auditing procedures.[24] The risk treatment plan here cannot wholly account for the nature of globalized business but steps should be taken to increase the system's overall transparency, monitoring and quality.

Conclusion

In brief, performing a risk assessment on an entire critical infrastructure sector is an immense undertaking. The challenges that exist in this sector alone are taxonomically diverse, geographically distributed and extremely complex. The successful navigation of the challenges discussed in this research note will require experts from nearly every functional area of the modern economy (law, finance, science and engineering, information technology, etc.). Enacting some of the treatment suggestions made in this note will simultaneously improve America's homeland defense efforts and address certain threats to the sector's competitiveness and profitability. The sector must embrace these rare opportunities that offer mutual benefit to both the public and the private sector participants operating in a shared critical infrastructure space.

ASA

Risk Consultants

References

[1] United States. Dept. of Homeland Security. *National Infrastructure Protection Plan Defense Industrial Base Snapshot*. 2007. Retrieved from http://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-defense-industrial-base-snapshot-2011.pdf

[2] Dept. of Homeland Security, pg. 1

[3] Bush, George W. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. 2003. Available at from https://www.dhs.gov/homeland-security-presidential-directive-7#1

[4] Bush, pg. 1

[5] Dept. Homeland Security, pg. 2

[6] Fortune 500. (2013). Fortune 500. Central News Network (CNN). Retrieved at http://money.cnn.com/magazines/fortune/fortune500/

[7] Fortune 500. (2013). Fortune 500. Central News Network (CNN). Retrieved at http://money.cnn.com/magazines/fortune/fortune500/

[8] The Commission on the Theft of American Intellectual Property. *The IP Commission Report.* United States: The National Bureau of Asian Research, 2013. pp. 1-6. Retrieved from http://ipcommission.org/report/IP_Commission_Report_052213.pdf

[9] Merle, Renae. "Boeing Agrees to Pay $615 Million Settlement." *The Washington Post.* 16 May 2004. http://www.washingtonpost.com/wp-dyn/content/article/2006/05/15/AR2006051500704.html

[10] The IP Commission Report, pg. 2

[11] The IP Commission Report, pg. 2

[12] The IP Commission Report, pg. 2

[13] The IP Commission Report, pg. 2

[14] The IP Commission Report, pg. 3

[15] The IP Commission Report, pg. 1

[16] The IP Commission Report, pg. 5

[17] Gettlemen, Jeffrey. "Enraged Mob in Falluja Kills 4 American Contractors." *The New York Times.* 31 March 2004. Retrieved from http://www.nytimes.com/2004/03/31/international/worldspecial/31CND-IRAQ.html

[18] Botwin, Brad. "Defense Industrial Base Assessments - Opportunities for Expanded Cooperation." Defense Manufacturing Conference. 28 November 2011. Conference Presentation, *n.p.* Retrieved from http://www.ndia.org/Divisions/Divisions/Manufacturing/Documents/bowtin.pdf

[19] "M1A1 Abrams Tank." *Military Factory*. Retrieved from http://www.militaryfactory.com/armor/detail.asp

[20] The IP Commission Report, pg. 1-5

[21] Botwin, pg. 11

[22] Botwin, pg. 11

[23] Botwin, pg. 11-12

[24] Botwin, pg. 12