Protecting Critical Technologies:

Intelligence Support for Technology Security

Protecting Critical Technologies: Intelligence Support for Technology Security

Abstract: Today, the most significant reform of the United States' arms transfer regime, since its inception following World War II, is presently underway. The current system of export controls has lumbered into a technical and mechanical labyrinth during and following the Cold War. The processes progressively frustrate the interagency, Congress, international partners, law enforcement officials, and U.S. industry, and the controls do not necessarily safeguard the most sensitive capabilities. In addition, the export controls lacks a systematic inclusion of intelligence support throughout the decision-making process. As the U.S. brings its arms transfer system into the 21st century through the current reform efforts, leaders have an ideal opportunity to ensure that meaningful intelligence support is fully integrated into the export control process. As the Director of National Intelligence (DNI) stands up National Intelligence Mission Managers based on country or issue-specific considerations, the intelligence community (IC) should establish a Technology Security Mission Manager to coordinate intelligence support requirements associated with the protection of U.S. critical technologies. The U.S. cannot tolerate the exploitation of vulnerabilities or the diversion of its best capabilities after the shooting begins. Unlike other threats, the damage our adversaries can inflict will not be known until the capability fails to function, is rendered obsolete through countermeasures, or is used against U.S. forces.

0314hrs, 10 June 2018, Straits of Taiwan. The VFA commander achieved altitude leading his squadron to intercept a wing of Chinese Sukhoi Su-30MK2 Flanker fighters. Although outnumbered four to one, the American pilots were confident in their aircraft's capabilities in what would be the first salvo of air-to-air missiles following China's invasion of Taiwan. After all, VFA-40 was equipped with the world's most advanced and expensive fighter, the F-35 Joint Strike Fighter. The U.S. aircraft automatically transmitted each fighter's real-time fuel consumption rates, location, and a myriad of other information to the USS Ronald Reagan. However, the returned "acknowledge" signal did not come from the Reagan, it came from a nondescript frigate off Meizhou Island. In a few milliseconds, communications from the squadron ceased, fuel shut-off valves closed, and pilot eject systems were disabled. The Reagan would lose its entire carrier air wing of F-35s and pilots in less than two hours. The U.S. Navy would learn too late that three years prior the Chinese had successfully accessed the network at Turkey's F-35 reprogramming center, discovered vulnerabilities in the F-35's source code, and developed exploitation software to bring down the aircraft without firing a shot.

If the scenario above sounds too far fetched, consider that the F-35's source code is 'the holy grail' for "controlling everything from weapons integration to radar to flight dynamics."[1] Then consider that hackers have stolen several terabytes of information related to the F-35's design and electronics systems; in certain instances the stolen information was encrypted so officials are not certain what data was compromised.[2] This vignette serves to highlight vulnerabilities to U.S. cutting-edge technology. Moreover, it points to only one of a myriad of constantly changing challenges to protecting U.S. technological advantages.

Robust intelligence support that goes beyond the intelligence community's (IC) current stove-piped structures and missions is required to assist in recognizing threats to U.S. critical technologies. The Director of National Intelligence (DNI) should established a Technology Security National Intelligence Mission Manager to coordinate the IC's support throughout the export control process and thus better ensure that U.S. critical technologies are adequately safeguarded.

[1] Jim Wolf, *Reuters*, "US to Withhold F-35 Fighter Software Source Code," 24 Nov 09, http://www.reuters.com/article/idUSTRE5AO01F20091125?pageNumber=1.

[2] U.S. officials suspect China was behind this theft. Siobhan Gorman, August Cole, and Yochi Dreazen, *Wall Street Journal*, "Computer Spies Breach Fighter-Jet Project," http://online.wsj.com/article/SB124027491029837401.html.

Protecting Critical Technologies: Intelligence Support for Technology Security

Background. The United States is the world's leader in advanced military technologies.[3] At one end of the spectrum, these technologies help to ensure that a U.S. soldier, airman, seaman, or marine does not have to fight a 'fair fight', at the other end they provide capabilities that ensure national survival, such as protection against weapons of mass destruction. The compromise of critical U.S. technologies has the potential to seriously endanger national security comparable to or greater than any threat from terrorism, yet, in comparison, IC support for technology security is rather underwhelming.

Of course the easiest way to protect advanced U.S. military technology would simply be to keep it under lock and key. However, it's in U.S. interests that international partners and allies also possess substantial military capabilities. Further, as the volatile post-cold war security environment drives the U.S. to engage increasingly with non-traditional partners, the associated precedent-setting transfers of sophisticated military capabilities to new partners makes protecting these capabilities even more challenging. The entities from which technology must be restricted is no longer limited to a handful of 'unfriendly states' but now includes an infinite number of potentially 'unfriendly individuals.' [4]

Consequently any U.S. export control system will be somewhat schizophrenic in nature. While there is a very pressing requirement to safeguard sensitive capabilities, there is often an opposing need to provide those same capabilities to friends and allies. This conflicting nature of export control is enduring. Conversely, the nature of what is being controlled – technology – and

[3] Examples include technologies that permit the targeting and killing of terrorists with unmanned drones from vast distances; technologies that produce the most advance missiles capable of intercepting ballistic missiles traveling at mach speed. These technologies are also going from the laboratories to the battlefield seemingly overnight.

[4] The revolution in information is not limited to computing power and communications. The revolution has led to the development of nanotechnologies, facilitating the end-item's mobility and concealment. Likewise, ever increasing computing power provides even the lowliest individual with the capability of modeling anything from new biological elements to nuclear weapons. The revolution has brought capabilities to and empowered non-state actors and individuals in arenas that were formally the sole purview of the state.

how it is controlled is ever-changing. U.S. military advantages are increasingly derived from technologies that are constantly evolving – improving – ostensibly at an exponential rate.[5]

Coupling the aforementioned trends with an arms transfer system designed for the cold war makes cooperation with foreign partners difficult and does not necessarily protect critical technologies.[6] President Barack Obama recognized these challenges and initiated a comprehensive interagency review to reform the export system. As the U.S. brings its arms transfer system into the 21st century through the current reform efforts, leaders have an ideal opportunity to ensure that meaningful intelligence support is fully integrated into the export control process.

Export Control Reform and Intelligence Support. The comprehensive review of export controls determined the current system required substantial reform in all four areas of control: what is controlled, how it's controlled, how the U.S. enforces those controls, and how the U.S. manages those controls.[7] Towards this end, the Administration envisions the establishment of a single control list, a single licensing authority, a single enforcement coordination agency, and a single information technology system.[8]

Despite the significance of U.S. advanced technologies and the potential impact of their vulnerabilities on national security, there is a near eerie absence of intelligence support in the proposed reforms. For the moment, IC support is limited to a senior liaison officer assigned to the single enforcement coordination agency with a focus on the traditional criminal aspects of

[5] The digitalization of technologies poses additional control challenges as it permits plans, software, source code, counter-measures, or any number of data parameters to be transmitted around the world with the click of a mouse.
[6] Robert Gates, Remarks by Secretary Gates to the Business Executives for National Security on the U.S. Export Control System, 20 Apr 10, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4613.

[7] Barak Obama, Video Remarks by the President to the Department of Commerce Annual Export Controls Update Conference, 30 August 2010.

[8] Whitehouse Fact Sheet, 20 Apr 10, http://www.whitehouse.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative.

illegal arms transfers.[9] However, there remains a readily apparent and, indeed, a pressing need for the IC to be integrated throughout the transfer process to provide critical functions in each of the core areas of export control.

Intelligence Support to U.S. Export Control		
Core Area		**Intelligence Requirement/Opportunities**

What We Control	Single Control List	• Assist in Determining Tier One Technology
		• Identify Critical Foreign/Advisory Requirements
		  o WMD Technologies
		  o Dual-Use / Commercial Off-the-Shelf
		• Identify Foreign Leading-Edge Technologies
		• Assess Foreign Availability of Tier One Technology

How We Control It	Single Licensing Agency	• Integrated with Policy-Maker for Responsive Intel Support
		• Validate End-Use and End-User
		  o Assess End-User Capability and Intent to Protect Sensitive US Technology
		  o Assess Diversion Risks
		• Provide Country or Technology Specific Risk Assessments
		• Leverage Transfers to Strategic Intelligence Requirements

How We Enforce Controls	Single Enforcement Coordination Center	• Identify Diversion of US Controlled Technologies • Identify Attempts to Defeat of US Anti-Tamper or Protection Schemes • Monitor Rouge-State Imports • Identify and Defeat Foreign Cyber Threats to Tier One Technologies • Identify Unauthorized Transfers • Implement Technology Counter-Intelligence Program
How We Manage our Controls	Single IT System	• Monitor Single IT System for Trends Analysis of Potential Threats, Diversions, or Unintended Consequences of US Transfers

Intelligence Support to the Single Control List. Currently the State Department has executive responsibility for the transfer of military capabilities that are on the Munitions List, and the Commerce Department oversees transfers of dual-use capabilities (items or services that have both a civilian and military function). The reform effort proposes a single control list that is

[9] Executive Order, dtd 9 Nov 10, "Export Coordination Enforcement Center."

tiered to allow the U.S. to build "higher walls" around the export of the most sensitive capabilities.[10]

The IC should assist the policy community in identifying higher tier technologies based on foreign capabilities and the risks they present to the U.S. Likewise, the IC should assist in identifying critical requirements for foreign governments' programs, such as their WMD programs. While they may not be viewed as critical technologies for the U.S., they may provide enabling capabilities that could advance an adversary's program.[11]

Intelligence Support to the Single Licensing Authority. As with the control list, licensing authorities are divided between the Departments of State and Commerce. Reform efforts include the creation of a Single Licensing Authority. If properly integrated, the IC could be a responsive asset in the development and execution of export control policies and decisions.[12]

This means moving beyond the traditional intelligence support to license reviews or assessments concerning a partner's ability to protect sensitive technology or data. While these functions are still extremely important, the establishment of a single licensing authority is an opportunity to better integrate intelligence into transfer decisions. Similarly, this integration could permit the IC to leverage certain transfers in a systematic process that may assist in meeting other strategic-level intelligence requirements or facilitate the development of

[10] Towards this end, the IC produced a National Intelligence Estimate (NIE) on Export Controls in August 2010 focusing primarily on traditional threats and risks from other state actors. A broader assessment into other non-traditional risks may have been more helpful considering the scope of the export control reform.

[11]For example, in 1998 Germany's export of 120 high-precision electronic switches to Iraq allegedly for 'spare parts' on medical equipment that pulverizes kidney stones are also used as nuclear triggers. Congressional testimony from Gary Milhollin, Director of the Wisconsin Project. http://www.wisconsinproject.org/pubs/testimonies/2000/5-26-00.htm. Furthermore, recognizing technology's constant changing nature requires the IC to provide an ever-changing assessment of 'the latest and the greatest' on a permanent basis.

[12] Wile serving as the Deputy Director for Analysis at the CIA, Secretary Gates noted the requirement for 'intelligence' is that it must be useful or 'actionable.' "The Intelligence community has to be right next to the policy maker, in that (the analyst) has to be at his elbow – that he has to understand what is on his mind. He has to understand what his future concerns are. He has to understand what is thehis agenda. He has to understand some of the initiatives that he is thinking about taking." James J. Wirtz, "The Intelligence-Policy Nexus", *Strategic Intelligence*, Edited by Loch Johnson, 2007, 142-3.

intelligence sharing arrangements with new foreign intelligence partners. To achieve this higher level of coordination, a senior representative from the DNI should serve in a prominent position on the Single Licensing Agency staff.[13]

Intelligence Support to the Export Coordination Enforcement Center. A November 2010 executive order established the Export Coordination Enforcement Center. While the order notes the importance of sharing intelligence for the enforcement of export control laws, there is a notable domestic bias in the mission of the center. It would also be valuable to utilize the IC for specific collection requirements on various foreign activities abroad which would identify the diversion or proliferation of controlled technologies.[14]

The ease with which information, including design and electronics system schematics of our most prized fighter aircraft as noted above, can be accessed and transferred around the world in seconds requires an evaluation of risks emanating from the cyber domain as well.[15] The IC has unique capabilities that can assist in enforcement efforts in this area too. The IC's full integration into the center with a broader focus than presently envisioned would improve enforcement capabilities.

[13] In addition, the administration could consider dual-hatting the IC official as the Technology Security Mission Manager.

[14] Abroad, the IC would have an important role in identifying attempts to defeat U.S. anti-tamper or protection schemes, unauthorized third party transfers (especially to rouge states), or any other range of threats to controlled technologies. Additionally, the IC could assist the export community by implementing a comprehensive Counter-Intelligence (CI) programs across the entire custody chain of certain critical technologies (from laboratories, to manufacturer, to transfer agents -i.e. foreign consignees [including electronic transfers], and ultimately to the end-users).

[15] The security assistance community also needs to take a much broader perspective on cyber threats. It must include cyber and other IT considerations and vulnerabilities in the development of protection plans. Plans, schematic, sensitive algorithms, anything that can be digitalized, can be transferred over the internet (maybe even unwittingly by an individual in business development). U.S. businesses that provide dual use technologies might not even understand or appreciate the impact of these illegal electronic correspondences. These risks require coordination with Program Offices and an effective Counter Intelligence program. The Military Services can not afford to address intelligence vulnerabilities in a stovepipe manner – they should coordinate with the entire IC.

Intelligence Support to the Single IT System. Currently, each stakeholder in the export control process manages its processes through separate IT systems. The administration plans on integrating these disparate systems into one single system. In addition to being the vehicle to managing transfer requests, this system could provide the IC with a powerful analytical tool to assist in identifying the acquisition trends of foreign governments, spot vulnerabilities for certain commodities, note unusual volume of certain technologies that may indicate diversion, or provide any number of assessments or information resulting from the consolidation of the various export control IT systems.

***Conclusion*.** The overarching theme of increasing intelligence support to the export control system highlights the opportunities and benefits to be gained by the IC's integration throughout the export process. The present reform efforts within the IC dovetail perfectly with reforms currently underway in the export control arena. As the DNI stands up National Intelligence Mission Managers along country or functional area considerations, a Technology Security Mission Manager should be created to coordinate intelligence support requirements associated with the protection of U.S. critical technologies.[16] The Technology Security Mission Manager should ensure the policy community's technology security intelligence requirements are properly integrated into the National Intelligence Priorities Framework (NIPF) and are adjusted to reflect the ever-changing nature of technology.[17] The systematic integration of intelligence support across all four core areas of export control would significantly enhance the government's ability to protect its most critical technologies.

[16] See DNI Instruction at http://www.dni.gov/electronic_reading_room/ICD_900.pdf. The mission-focused concept of this IC reform efforts calls for management and structure based on national security *missions* rather than *collection.* The mission manager concept is ideally suited for the rapidly changing technology environment and the threats the U.S. faces in trying to protect its technological lead. Larry Kindsvater, "The Need to Reorganize the Intelligence Community," *Intelligence and the National Security Strategist*, ed., Roger George and Robert Kline, 57 and 60, 2006.

[17] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 2009, 57-9.

The U.S. cannot afford to discover the exploitation of vulnerabilities or the diversion of its best capabilities after the shooting begins. Unlike other threats, the damage our adversaries can inflict will not be known until the capability fails to function, is rendered obsolete through countermeasures, or is used against U.S. forces. An integration of IC support into the export control process will significantly mitigate the risks of such potentially devastating consequences.

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR POLICY

BIOGRAPHY

Steve Coonen

Steve Coonen serves as a Senior Foreign Affairs Advisor at the Defense Technology Security Administration (DTSA) in the Office of the Under Secretary of Defense for Policy. He was recently selected to participate in the Defense Senior Leader Development Program (DSLDP) and is currently attending the National War College.

stephen.coonen@dtsa.mil
(703) 842-7504