Protecting Partners or Preserving Fiefdoms? How to Reform Counterintelligence Outreach to Industry

BY DARREN E. TROMBLAY | OCTOBER 2017

It's time for a new approach to counterintelligence outreach to the commercial sector—one that focuses more on recognizing and responding to indicators of the threat, less on turning to investigators once the damage has already been done.

U.S. industry is increasingly independent of federal government direction in its creation of new knowledge and capabilities. Nonetheless, the outputs of industry support the United States' ability to maintain elements of its national power. Consequently, industry is in the crosshairs of not only foreign competitors, but also of foreign intelligence services that seek to surreptitiously obtain valuable knowledge and other intellectual property. This is an unfair fight. It is further complicated by the fact that both adversaries and allies alike have directed their intelligence resources against U.S. industry.

Although the U.S. government has attempted to partner with the private sector on counterintelligence (CI) awareness and response, these efforts have been plagued by a limited concept of which industry sectors are at risk, inconsistency in programs, and redundancies across agencies. Moreover, the U.S. intelligence community is already being asked to do more with less.

It is time for a new approach to the important function of counterintelligence outreach to the commercial sector. Such an approach must focus more on recognizing and responding to indicators of the threat, less on turning to investigators once the damage has already been done. Counterintelligence—in the theoretical sense—means preventing an adversary's intelligence services from acquiring an information advantage. While U.S. government agencies such as the Federal Bureau of Investigation, the Defense Security Service, the Department of Commerce, and the Department of Homeland Security make a valiant effort to disrupt criminal activities, they are only part of the solution. Missing from this approach is assistance to industries trying to navigate technically legal but unscrupulous

activities such as China's mercantilist approach to doing business—which can do long-term damage not just to U.S. companies, but also to U.S. strategic interests that are supported by the capabilities U.S. companies develop.[1] The final necessary piece of a solution is enlisting the active participation of the private-sector entities at risk, since they are the first line of defense and best postured to identify anomalies.

To accomplish all this, the Trump administration should establish an interagency hub to consolidate existing counterintelligence outreach programs. The hub should not simply be an aggregation of programs, but, like the National Endowment for Democracy, an entity that focuses resources on achieving a strategic outcome—preservation of U.S. commercial ingenuity. This hub should be structured as a public-private partnership that incorporates industry, which is increasingly the front line of defense against foreign intelligence activities, as a contributing partner, rather than simply a recipient of government services. It should work to connect specific companies that have encountered foreign threats with the appropriate national security agencies that are best suited to disrupting these threats. Counterintelligence agencies should use this hub as an honest broker between the national security community and the private sector, which is an increasingly significant contributor to elements of U.S. national power. It must be capable of translating the community's concerns into publicly releasable explanations of sector-specific threats.

The Trump administration should establish an interagency hub to consolidate existing counterintelligence outreach programs.

This report first discusses the concept of counterintelligence. It examines the role of the private sector in protecting its own intellectual assets. It then examines the history of U.S. government efforts and the limitations and problems with these efforts. The report focuses on a key challenge: the changing priorities of the FBI and the negative consequences for commercial counterintelligence efforts. It then discusses the challenges of redundancy of counterintelligence efforts across the U.S. national security community. Finally, it discusses needed government and industry changes to better protect U.S. commercial knowledge assets.

COUNTERINTELLIGENCE AS A CONCEPT

Over the last decade, the commercial sector has been a routine target of foreign state and non-state actors. In 2017 alone, several countries made headlines because of illegal attempts to acquire information and technology. For instance, in April 2017, a Chinese national pled guilty to trying to provide the Chinese government with export-restricted high-grade carbon fiber, which is primarily used in aerospace and military applications.[2] Approximately a month later, four U.S. citizens were charged with conspiring to steal trade secrets from a U.S. business, on behalf of a Chinese company that was involved with manufacturing what the U.S. Department of Justice characterized as a "high-performance, naval-grade product" for military and civilian uses.[3] However, China is not the only country to engage in nefarious activity against the U.S. private sector. In July 2017, U.S. officials identified Russian government hackers as having conducted cyber-intrusions into the business systems of U.S. nuclear power and other energy companies.[4] Russia's malfeasance should not come as a surprise. As early as 1991, then-Russian intelligence

chief, Yevgeny Primakov suggested that Russian intelligence would shift to the commercial sphere.[5]

Counterintelligence is not just about spies—it is about preventing the transfer or corruption of knowledge. Transfer of knowledge—regardless of whether the topic is policy, corporate strategy, or technology—changes an actor's informational advantage. Acquisition of information supports incisive decision making and creation of new capabilities with which to implement those decisions. Loss of information results in a setback for an actor's position vis-à-vis competitors, adversaries, and sometimes even allies. Corruption of knowledge through influence campaigns or technical manipulation of data similarly degrades an actor's informational advantage. Many governments have professionalized this process of acquiring or corrupting knowledge in their intelligence services. However, one need not be affiliated with the CIA, KGB (Russia), or MSS (China) to collect information that enhances the position of a state or non-state actor. The increasingly transnational nature of corporate America brings with it the associated growth in vulnerability to exploitation by a variety of foreign state and non-state actors seeking to enhance their relative position vis-à-vis the United States.

The problem of information and technology transfer is not just a detriment to U.S. strategic capability, it is also an attack of staggering proportions on the American economy. Estimates of loss vary but they are all sobering. In 2013, the Center for Strategic and International Studies assessed that economic espionage, including cyber activity, cost the United States between $24 billion and $120 billion per year.[6] The Commission on the Theft of Intellectual Property, which former Director of National Intelligence Dennis C. Blair and former Ambassador Jon M. Huntsman Jr. chaired, estimated that the cost to the U.S. economy of international intellectual property theft amounted to more than $300 billion annually.[7] The cost is difficult to estimate because it must include not only the cost of research and development (R&D) and other product development costs and diminished market share but also lost opportunities due to future, competing technologies based on the sunk R&D costs. Regardless of the rubric one uses for estimates, a 2013 statement by then-Director of the National Security, Keith Alexander, (who was double-hatted as the head of Cyber Command) calling economic espionage against the United States "the greatest transfer of wealth in human history" sums up the immensity of the problem.[8]

Cybersecurity has often been treated in a vacuum (the FBI, for instance, has created a cyber division apart from its counterintelligence and criminal investigative components) when in reality it is a subset of counterintelligence. Regardless of whether a threat actor is foreign or domestic, or stems from insider behavior or an external cyberthreat, its initial objective is to acquire an informational advantage. A hack to obtain proprietary data from the government or private sector contributes to the capabilities of the hack's sponsor. Even cyber events that trigger a physical crisis start with collection. A threat actor must first reconnoiter the vulnerability that it wants to attack before it can exploit this newly acquired information to degrade U.S. equities, which have ranged from elements of critical

infrastructure (e.g. the electrical grid, nuclear power plants, dams, etc.) to content produced by the entertainment industry (*a la* North Korea's hack of Sony).[9]

The Evolving Private and Public Roles in Technology Development

The capabilities inherent in the U.S. private sector are increasingly important to preserving elements of American national power. The paradigm of government-driven research and development, especially as it relates to defense capabilities and leads to commercial spin-off, has been increasingly obsolescent since the Cold War ended. Furthermore, "hard power"—military applications—is only one implement with which states can produce desired outcomes. The non-defense commercial sector is a now a significant contributor not only to technological innovation that is of value to national security, but also to the fields of economics and information—two other essential aspects of national power. Even the fourth element of national power, diplomacy, is no longer limited to the government. Multinational firms, academic institutions, and non-governmental organizations act with independence on the global stage. They also develop media platforms essential to public diplomacy.

The capabilities inherent in the U.S. private sector are increasingly important to preserving elements of national power.

Washington is no longer the principal patron of the U.S. technology industry but, instead, simply another customer. This trend became apparent in 1999 when the CIA launched In-Q-Tel as a private, nonprofit firm to provide venture capital to small companies developing technologies of interest to the U.S. intelligence community.[10] More recently, the U.S. Department of Defense established its Defense Innovation Unit Experimental (DIUX) in Silicon Valley, to identify and better incorporate emerging and breakthrough technologies.[11] The Department of Homeland Security, which, through its Science and Technology Director, is responsible for delivering effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise, has similarly demonstrated a reliance on not just dedicated defense and homeland security firms, but also on the broader technology industry. As of 2015, DHS established its office to recruit talent from the tech sector and to build relationships with industry.[12] All of these developments are acknowledgements that the U.S. government has become more of an adopter and adapter, rather than an originator, of cutting-edge applications.

The United States government's role as a customer also means that it is in competition with other bidders—including entities that serve as proxies for adversarial governments. Through state-backed foreign direct investment, hostile governments (e.g. China) have successfully acquired many U.S. commercial ventures and have unsuccessfully tried to acquire many more.[13] Companies from other countries, including China, have also made "greenfield" investments on U.S. soil, in an effort to leverage local talent. For instance, Baidu—a Chinese search engine—launched an artificial intelligence laboratory in Sunnyvale, CA.[14] Additionally, U.S. companies seeking markets abroad have sometimes been forced to provide geopolitical enemies with proprietary information in order to enter national markets. China has consistently used this transactional approach, even though it violates World Trade Organization rules.[15] Russia has also demonstrated its willingness to employ a similar method of acquisition. According to a June 2017 Reuters investigation,

Moscow has issued demands that American information technology companies allow the government to examine the source code of software products.[16]

The History of Federal Counterintelligence Efforts

The federal government has a long history in commercial counterintelligence, but as noted below, the engagement has been episodic, with the FBI, most notably establishing, dismantling, and then re-establishing multiple programs to engage the private sector since the early 1940s.

Plant Protection Program

The FBI's Plant Protection Program (PPP) is an early example of counterintelligence outreach. As European tensions became open hostilities, the FBI initiated the PPP in September 1939.[17] This program, as outlined in the Bureau guidance, would instruct manufacturing plant managers on topics including: duties and responsibilities of plant protection employees; the role of the FBI in plant protection and the cooperative functions of the FBI; discipline, loyalty, tact, alertness and appearance; promptness in reporting irregularities; note taking on the part of plant employees; searches of persons; searches of places; fingerprinting; protection of the scene of the crime; developing informants; firearms training; patrol work; supervising the visitors of the plant; espionage and sabotage methods; personal descriptions; bombs and explosives; and arson.[18]

The FBI's approach to plants was twofold. At an immediate, operational level, special agents inspected sites, identified vulnerabilities and provided recommendations on how to mitigate threats.[19] The Bureau considered it to be:

> highly desirable for Agents during the survey to discuss with the plant protection officials the apparent weaknesses of the present plant protection set-up. This procedure affords the Agent an opportunity of ascertaining what steps have been taken in the past to attempt to improve the protection organization and the results of these attempts. This procedure affords the Agent an opportunity of receiving suggestions from the plant protection officials.[20]

Engagement of plant management in longer-term awareness of potential threats complemented more immediately oriented actions. The FBI also distributed 21,000 copies of a confidential booklet, which outlined the basic principles of protection against espionage and sabotage, to reliable plant officials and representatives of public utilities, railroads, and steamship companies (the sectors that would, today, be called "critical infrastructure").[21] In 1939, the Bureau's then-Director, J. Edgar Hoover, indicated that this manual was the first-ever U.S. iteration of such guidance.[22] In mid-1940, the FBI's Executive Conference (comprised of the Bureau's assistant directors) determined that the booklet, *Suggestions for Protection of Industrial Facilities*, should only be given out when requested by industry officials. These books, provided after the plant inspection, would provide the special agent in charge (SAC)—the head of an FBI field office—with "the basis for continuing the contact with the plants."[23] Furthermore, the Bureau was concerned that if the books circulated too widely and a plant obtained one prior to a plant survey, the

plant might put into effect recommendations "which an Agent would be in a better position to make to more effectively protect the plant's facilities."[24] The Bureau's relationships with plant managers were of a distinctly liaison nature. According to a 1940 memorandum for the Director, which criticized certain field offices' counting general managers and officials as informants, "The [Executive] Conference also instructed that the names of officials of the plants not be included as informants and that the field should be advised that these officials are to be considered as contacts . . . ."[25]

Agents who participated in plant protection work came from both HQ and various field offices. These individuals received training during a several-day in-service on topics including: Bureau policy on plant protection; specific examples of methods and types of espionage and sabotage reported to the Bureau to date; and laboratory aspects of plant protection. These agents were also advised that there were specific topics that should not ever be discussed with plant officials. There were: employee relationships, alien personnel, spot searches, fingerprinting, telephone tapping and monitoring, labor organizations, and explosives.[26]

The federal government has a long history in commercial counterintelligence, but the engagement has been episodic.

Possibly because of wartime exigencies, the Bureau reduced and ultimately ended its work in the field of plant protection. Starting in 1940, the FBI's duties prevented personnel from being able to teach specific subjects.[27] By late 1942, the FBI was no longer conducting plant surveys. The Executive Conference afforded consideration to reducing instruction for new agents on plant survey matters from eight hours to two hours, since their responsibility in this area would be the general problem of plant surveys and the Bureau's policies. Thus, the agents could discuss this subject sufficiently with local authorities and individuals in industry.[28] It is interesting to note that the Bureau continued to utilize agents with expertise in this area for substantive work domestically. In 1944, an agent "trained in plant protection survey" examined each of the Bureau's radio installation to make security recommendations.[29]

From its outset, the PPP was an enterprise that served an interagency constituency. The Army and Navy designated the key manufacturing establishments that were vital to the national defense program.[30] The list of priority establishments, which the Bureau received from the armed services, included 430 facilities of concern. Additionally, the Army and Navy identified another 12,000 plants that would come under the PPP's purview in the event of war.[31] The FBI furnished the results of the plant surveys to the Office of Naval Intelligence or the Military Intelligence Division, depending on which service had the contract with the industrial plant.[32]

Development of Espionage, Counterintelligence, and Counterterrorism Awareness (DECA)

The FBI's Development of Espionage, Counterintelligence and Counterterrorism Awareness (DECA) program was a successor to the Plant Protection Program. There is no indication that the FBI had a formalized outreach program during the interregnum between the end of the PPP and DECA's beginning. DECA, which the Bureau officially launched in 1978, was based on a project that a field office had initiated in 1976.[33] The

field office's initiative involved systematically contacting all of the defense contractors within the office's area of responsibility. This alerted contractors to the threat that hostile intelligence services posed and provided the private-sector entities with a point of contact should unusual activity come to their attention.[34] With the program, the FBI's resources were linked with the security measures employed by U.S. defense contractors and focused on the targets of foreign intelligence service activity.[35] (DECA overlapped with the Cold War, when the Soviet Union was the primary threat to the United States, and continued into the post-Cold War early 1990s, which then-Director of Central Intelligence R. James Woolsey likened to a "jungle filled with a bewildering variety of poisonous snakes."[36]) As an FBI official described to Congress in 1988, DECA "seeks to heighten the awareness of corporate executives and their employees to the hostile intelligence services threat."[37]

The DECA program's mission broadened throughout its existence. For instance, the FBI realized that much of the sensitive information of value to foreign entities was not always classified, defense information. Much information of interest to adversaries was unclassified and frequently publicly available. The FBI began to focus more on emerging technologies such as genetic engineering.[38] As the program went on, the FBI also focused less on interacting with the facility security officers of U.S. companies and more directly with the rank and file employees, especially those that had direct contact with foreign agents. [39] (Opportunities for such contact range from foreign visits of U.S. facilities to business travel abroad.) DECA created an opportunity for a true give and take relationship between the FBI and industry. The FBI was able to educate companies and their employees about threats as well as receive information and investigative leads concerning foreign governments' attempts to illicitly collect economic and technological information.[40]

Components at FBI headquarters, the Bureau's field offices, and other national security agencies contributed expertise and resources to the DECA effort. Once it was adopted nationally in 1978, DECA was implemented across all field offices. In 1990, the FBI appointed a national DECA coordinator and established a national DECA advisory committee, which included DECA coordinators from the FBI's larger field offices.[41] At the field level, DECA coordinators in each of the FBI's field offices had regular liaison with companies within the field offices territory. Each DECA coordinator aimed to assist businesses in understanding and recognizing foreign economic and espionage threats as well as the tradecraft that the foreign governments employed to collect intelligence.[42] DECA also became a platform from which multiple agencies could contribute to counterintelligence. For instance, the National Counterintelligence Center (NACIC) worked with the FBI through the DECA program.[43] Additionally, the Central Intelligence Agency (CIA) provided information to the FBI by way of the DECA program.[44]

The DECA program had a broad mandate. Over the course of its existence, the program expanded to include firms that were not engaged in classified government contracts.[45] In 1995, the U.S. National Counterintelligence Center provided an indication of the scope of the foreign threat to U.S. industry at the time of the DECA program. According to the Center, the industries that were most often the targets of economic espionage and other

collection activities included biotechnology; aerospace; telecommunications; information technology; advanced transportation and engine technology; advanced materials and coatings—including "stealth" technologies; energy research; manufacturing processes; and semiconductors, as well as the expected defense and armaments technology.[46] No wonder that, in fiscal years 1993 and 1994, the FBI briefed nearly 20,000 companies.[47]

Awareness of National Security Issues and Response (ANSIR)

Consistent with its developing involvement with industry outreach, the FBI established the Awareness of National Security Issues and Response (ANSIR) program in 1996 to replace DECA. ANSIR was a response to the changing dynamics of a post-Cold War environment. According to the Deputy Assistant Director responsible for the program, these factors included foreign intelligence services' expansion of targeting to include unclassified private-sector proprietary economic information; the escalated threat of terrorist attacks on American interests; and the problems of computer intrusion and viruses.[48] In additional to traditional defense-related information, ANSIR addressed clandestine targeting or acquisition of sensitive financial, trade or economic policy information, and proprietary economic information. ANSIR tended to focus on violations of the Economic Espionage Act (EEA).[49] The U.S. Congress passed the EEA in 1996 to address the growing problem of trade secret theft. In its first provision, the EEA addresses the theft of trade secrets to benefit a foreign government. The second provision of the EEA criminalizes the commercial theft of trade secrets regardless of the theft's beneficiary.[50]

Congress passed the Economic Espionage Act in 1996 to address the growing problem of trade secret theft.

ANSIR was innovative in several ways. It was the first effort by the U.S. government to provide national security threat information to individual U.S. corporations with critical technologies or sensitive economic information that foreign government or organizations might target.[51] Furthermore, it contained a concept that could have helped industry to become a force multiplier in counterintelligence. Specifically, the ANSIR program gave industry representatives guidance about the "techniques of espionage" to help them identify their own vulnerabilities.[52] If implemented effectively by companies, this knowledge would have helped the private sector to act preventively, rather than simply turning to the Bureau once damage had already occurred.

Unfortunately, ANSIR's ambitious agenda was not matched by the resources needed to implement it effectively. To be sure, up to 40,000 U.S. corporate security directors and executives, law enforcement personnel, and other government agencies received warning information through this program.[53] However, as of 2001, the entire program was overseen by a single supervisory special agent (the lowest rung of FBI management) in the National Security Division at FBI Headquarters.[54] Each of the FBI's 56 field offices had a special agent who coordinated the ANSIR program locally. However, this function was an ancillary duty that was not supposed to take more than 10 percent of the agent's time.[55] Despite the limited time that each agent could afford the program, they were expected to meet regularly with industry leaders and security directors.[56] It was mandatory that a special agent—as opposed to an intelligence analyst or support employee—fill the role, since, according to the deputy assistant director in charge of the program, "decades of

experience with the ANSIR audience has shown that the private sector prefers discussing national security issues with an individual who has operational experience."[57] The program's limited resources (an FBI deputy assistant director reported to Congress that ANSIR, "by any measurement of government programs is a very small one"), coupled with the Bureau's emphasis on counterterrorism in the aftermath of the September 11 attacks, likely contributed to ANSIR's disappearance.

Counterintelligence Strategic Partnerships (CSP)

By 2005, the FBI had reinvented its approach to engaging the private sector. Its Counterintelligence Strategic Partnerships (CSP) program was the successor to the Plant Protection Program, DECA, and ANSIR. According to information provided by the FBI on its publicly available website, as of 2017, economic espionage was the second highest priority for the Bureau, just behind fighting terrorism.[58] The CSP was designed as a network of loose partnerships between individual regional FBI field office and the businesses, academic institutions, think tanks and trade organizations operating within the field office area of responsibility.[59] As of 2014, it had more than 15,000 contacts in these sectors.[60] The program consisted of approximately 80 special agents who were well-versed in counterintelligence.[61] Each of the 56 FBI offices has designated at least one, and sometimes multiple, agents who specialized in conducting outreach activities regarding counterintelligence and counter espionage matters. These agents provided security awareness training and dealt with threats and concerns from the Bureau's external partners. The CSP program also provided a platform for interagency collaboration on shared areas of concern. One example was the creation of a Defense Security Service (DSS) / FBI Strategic Partnership Task Force at the Washington Field Office, "established to include CI outreach to industry and create opportunities for the two entities to work together in countering the threat to cleared industry through information sharing and joint support efforts."[62]

The CSP made progress in promoting security awareness, especially in the area of economic espionage, across a variety of industries. Whereas previous outreach efforts emphasized the defense industry, where contractors had security clearances, as a target for economic espionage, the SPC expanded the Bureau's outreach to industries that were unaccustomed to thinking about foreign adversaries and had typically little interaction with the FBI. The agriculture and seed industry, for instance, was caught off guard in 2012 when the FBI arrested several Chinese individuals for digging up corn seeds from a test plot in Iowa.[63] The culprits were apprehended on a plane to China with seeds hidden in their luggage in packages disguised to look like popcorn. News of these cases shocked the industry and created a desire to interface more closely with the FBI.

Office of Private Sector (OoPS)

The CSP program—although it was simply the latest iteration of previous initiatives—appeared to be moving in the right direction in aligning the FBI with the realities of 21st century industry and global competition. The Bureau again reinvented its outreach with the creation of its Office of Private Sector (OoPS) in 2014.[64] The OoPS was supposed to

reflect Director Comey's desire to remain "ahead of the threat through leadership, agility and integration."[65] According to its publicly released fact sheet, OoPS would align and coordinate key private-sector engagement programs within the FBI. Unfortunately, it included another "baby with the bathwater" moment with its announcement that it would "redesign legacy partnerships." Although the CSP program pre-dated the formation of OoPS, the publicly released OoPS fact sheet makes no mention of the partnership.[66] The jury is still out on whether OoPS is just another exercise in reinvention that will be supplanted by yet another initiative, becoming merely another chapter in the FBI's disjointed history of outreach.

InfraGard

The history of the FBI's InfraGard program highlights the problem of outreach in the cybersecurity field. In 1996, the FBI's Cleveland Field Office launched InfraGard, in conjunction with subject matter experts from local industry and academia, to focus on cyber and physical security issues.[67] However, the FBI was not first to the scene on cyber issues. In 1984, the U.S. Secret Service (USSS), which, at the time, was under the auspices of the Department of Treasury, had received authority to investigate computer crimes. Mission overlap was perhaps inevitable since cyber is not an actor—it is a vector that can be weaponized by any number of threat entities (which, in turn, fall under the jurisdiction of multiple agencies).

The massive reorganization that produced the Department of Homeland Security again highlighted the government's inability to easily divide responsibilities in the field of cyber-related liaison.

Despite the lack of clarity about responsibilities, the FBI built Infragard into a national program. With the 1998 "Presidential Decision Directive 63 on Critical Infrastructure Protection" as the impetus, the Bureau established the National Infrastructure Protection Center (NIPC) and created a National Infrastructure Protection and Computer Intrusion Program (NIPCIP) with regional squads in 16 field offices.[68] Infragard became a function of the NIPC (which, in 1999, became part of the FBI's Counterterrorism Division).[69] As part of NIPC, Infragard was supposed to be a national-level program with direct private-sector contacts and the formation of member chapters within each FBI field office jurisdiction.[70] Unfortunately, the NIPC's liaison activities almost immediately fell victim to the same paucity of resources that had plagued previous initiatives. The NIPC, a headquarters entity, did not have agents in the field. Consequently, field offices were forced to balance the NIPC's requests against the more pressing exigencies that ongoing investigations posed.[71] Infragard was also not the only responsibility that NIPC levied on the field. The portfolio for agents handling NIPC matters also included computer intrusions, viruses, and liaison with state and local officials.[72] By 2001, NIPC was already characterized by poor morale, inadequate staffing and a lack of expertise.[73]

The massive government reorganization that produced the Department of Homeland Security again highlighted the government's inability to easily divide responsibilities in the field of cyber-related liaison. DHS's National Cyber Security Division replaced the NIPC in 2003.[74] However, this shakeup threatened to cause the same sort of disruption that had characterized the reinvention of other counterintelligence programs. Senator Charles Grassley (R-IA) expressed concern that the decision to move NIPC would "destroy the

fragile trust" that had formed between the Center and the private sector.[75] Senator Grassley's appropriate concern went unheeded. However, the FBI maintained control of the Infragard program, which it moved under the newly created Cyber Division.

For the time being, Infragard remains under the auspices of the Cyber Division. As of 2014, there were 25,863 active members including business executives, academics, and state and local law enforcement.[76] There is a least one InfraGard chapter in the territory of each of FBI's 56 field offices. The regional chapter meetings promote trusted discussions of member vulnerabilities as well as the needs of the FBI. The program consists of 17 infrastructure categories, including agriculture and food, energy, and defense.[77] InfraGard allows subject matter experts from these sectors to exchange information and discuss vulnerabilities among themselves and with the U.S. intelligence community. The FBI Cyber Division's National Industry Partnership Unit uses the Infragard network to facilitate the transfer of information between the public and private sectors.[78] However, Infragard is among the "legacy partnerships" that OoPS has explicitly identified for redesign.[79] This does not bode well for consistency.

Defense Security Service

The Department of Defense's Defense Security Service (DSS) has implemented multiple measures to protect industries that were responsible for doing work under the auspices of security clearances from compromise by foreign entities. It created a course for the National Industrial Security Program (NISP) community on foreign ownership and control issues (FOCI) and hosted conferences on these issues.[80] (Executive Order 12829 of 1993 established NISP to safeguard Federal Government classified information that is released to contractors, licenses, and grantees of the United States Government.) Furthermore, DSS provides tailored assessments, known as the "Gray Torch," which are meant to strengthen a company's understanding of the nature of the foreign intelligence threat and to identify and recognize unlawful attempts to acquire U.S. technology developed or produced in the facilities operating under the NISP.[81] (This is similar to the function with which the military entrusted the FBI's PPP in 1939.) DSS has also gone so far as to exchange personnel with companies under its purview. In 2009, it initiated its Partnership with Industry Program, which involved the exchange of security personnel for a week to improve communications and give the private sector a better understanding of DSS' mission.[82] The Counterintelligence Partnership with Cleared Industry Program, which began in 2012, gives companies the opportunity to work directly with the DSS Counterintelligence Directorate. Participants provide value to DSS through discussion of pitfalls, successes, best practices and lessons learned in a non-attribution environment. Companies benefit from access to DSS information systems that they can use to analyze threat information of relevance to their activities.[83]

Department of Commerce

Within the Department of Commerce, the Bureau of Industry and Security (BIS) engages in a variety of outreach activities. Its Project GUARDIAN contacts U.S. manufacturers and exporters that handle technologies and goods that specific proliferation networks are

targeting. A proliferation network, according to a report of the Government Accountability Office, uses business and commercial practices to circumvent national and international restrictions against procurement of technologies by entities prohibited from obtaining those technologies. It apprises them of the acquisition threat and solicits cooperation in identifying and responding to suspicious purchase requests.[84] In 2014, BIS initiated 103 Project GUARDIAN outreach contacts and developed 206 leads.[85] Additionally, BIS conducts multiple seminars, throughout the United States, for the high-technology community, exporters, and re-exporters. These seminars provide education about export controls.[86] BIS also reaches representatives of technology firms through its Annual Export Control Forum.[87] Academia has expressed concern about deemed exports, due to the impact that these regulations would have on foreign students' research. Consequently, BIS has been working with non-profit organizations associated with university research programs to explain deemed export regulations.[88]

One "Project Shield America" success occurred in 2009, when an industry outreach event identified a dual Canadian/Iranian citizen who was attempting to acquire pressure transducers from a U.S. company.

Department of Homeland Security

DHS has its own outreach program under the auspices of Immigration and Customs Enforcement (ICE). ICE's "Project Shield America" seeks to enlist the assistance and cooperation of companies involved with the export of U.S.-origin strategic technologies and munitions items, as well as academics who study these and other strategic fields.[89] It includes presentations for U.S. manufacturers and exporters of arms and sensitive technology. These presentations include information about export laws, licensing issues, and "red flag" indicators associated with illegal procurement and best-practices for compliance with government agencies. One Project Shield America success occurred in 2009, when an industry outreach event identified a dual Canadian/Iranian citizen who was attempting to acquire pressure transducers from a U.S. company.[90] Another success occurred when Homeland Security Investigations learned of an online, illegal purveyor of export-restricted software products during a private industry outreach meeting.[91] DHS inherited an outreach concept from at least one component agency. Prior to absorption into DHS, the U.S. Customs Service, under the Department of Treasury, initiated Project GEMINI, which apprised U.S. businesses about export requirements and encouraged their reporting of attempts to illegally acquire or export sensitive military equipment or technologies.[92] Although Project GEMINI served U.S. government interests, it also, as a byproduct, encouraged companies to be more vigilant about the loss of sensitive technologies.

Elements of cybersecurity—potentially overlapping with the FBI's Infragard program—also fall under the DHS bailiwick, in the form the Department's responsibility for the U.S. Computer Emergency Readiness Team (US-CERT). Initiated in 2003, US-CERT provides a web-based collaborative system that facilitates sharing of sensitive cyber-related information with multiple participants, including members of industry.[93] Furthermore, the US-CERT public website provides government, the private sector, and the public with information that serves to help protect information systems and infrastructures.[94]

LIMITATIONS OF FEDERAL COUNTERINTELLIGENCE EFFORTS

Unfortunately, even with this litany of programs, the U.S. federal government is not well-postured to provide meaningful assistance to the private sector. It has developed an aggregation of counterintelligence awareness programs over decades. However, these initiatives are characterized by two factors that undercut their efficacy. First, as noted above, they have suffered from inconsistent implementation. This inconsistency of effort has impeded the ability to establish long-term meaningful, mutually-beneficial relationships. Furthermore, aspects of outreach are duplicated across multiple agencies. Although the FBI is the lead agency for counterintelligence, the Department of Homeland Security and the Defense Investigative Service also field programs and this duplication of efforts creates a confusing environment that may make it more difficult for companies to work effectively with government.

Inconsistency of Federal Effort

The FBI, as the lead U.S. government agency for counterintelligence issues in the domestic setting, is the natural sponsor for counterintelligence outreach. However, it has demonstrated an inconsistent approach to this function—progressing from the Plant Protection Program, to the Development of Espionage, Counterintelligence, and Counterterrorism Awareness (DECA), to the Awareness of National Security Issues and Response (ANSIR), to Counterintelligence Strategic Partnerships, to its current Office of Private Sector (which truncates, acronymically, to the unfortunate 'OoPS'). Drs. Michael Stouder and Scott Gallagher have pointed out "relationships are a critical [counterintelligence] resource."[95] However, it is difficult to establish meaningful relationships if the CI outreach component is in a regular state of churn.

The FBI is hampered by an overly broad mission, which causes shifts in focus as new exigencies arise. These shifts in focus bring with them a reallocation of resources. This can have a detrimental impact on programs, like the already-small ANSIR, when an urgent national security crisis, such as the September 11 attacks occurs. This combination of factors leads to inconsistent attention to initiatives such as counterintelligence liaison with the private sector which, although not addressing an immediate threat to life and limb, can protect strategically significant U.S. R&D capabilities. Consistency, however, is essential to the success of liaison initiatives. For private-sector entities to become useful partners to the government, they need to view liaison relationships as part of the status-quo; a routine part of doing business.

Historically, this problem has been apparent in reassignment of personnel. At the end of the Cold War, the FBI moved 300 special agents from its foreign counterintelligence program to its violent crime and major offenders program.[96] This was in spite of the fact that then-FBI Director William Sessions acknowledged that the impending decade was one of "unprecedented political transitions" and that the FBI had to determine where the greatest threats existed.[97] Political transitions are of distinct CI concern, since governments field intelligence services. Despite Sessions' uncertainty about the geopolitical outcomes that would define the CI landscape, he nonetheless moved resources away from CI. Then,

in the wake of the attacks of September 11, 2001, then-FBI Director Robert Mueller III moved 2,000 agents away from criminal issues—primarily narcotics and health care investigations—to national security matters, with an emphasis on counterterrorism.[98] However, only a few years later, the Bureau found itself shifting resources from counterterrorism to counterintelligence and assigning new agents to work against Chinese spies.[99] Although this was a positive contribution to CI resources, it also demonstrated the impermanence of assignments, a condition that could just as easily diminish the CI program in the future, as it had done under Sessions.

The FBI has, unfortunately codified a permanent state of change into the Threat Review and Prioritization (TRP) process, its current organizing rubric. TRP is an annual process that directs the allocation of resources to the highest rated threats.[100] Operational divisions and field offices are required to identify and prioritize national threat issues and develop strategies to mitigate these threats. As its title suggests, TRP focuses on threats, at the expense of understanding the landscape from which threats originate. Consequently, according to the 2015 9/11 Commission Review, the process gave little attention to emerging threats.[101] This shortcoming leaves the FBI ill-equipped to identify indicators of new issues until they become full-blown threats. The Bureau has been down this road before: moving agents away from national security issues in the early 1990s did not halt the growth of terrorism, it just distracted the FBI from the problem of terrorism (even as the threat—from both foreign and domestic terrorists—became increasingly manifest throughout the decade); similarly, moving agents to counterterrorism assignments in the early 2000s, did not end the threat from Chinese spies, to which the Bureau then had to allocate resources as the decade progressed. Dedication of resources to programs is necessary if the Bureau, or any intelligence service, is going to understand how an existing threat is evolving and how to disrupt this evolution before it can cause damage in new ways. But that dedication cannot be fleeting.

The FBI is hampered by an overly broad mission, which causes shifts in focus as new exigencies arise.

Despite its actions, the FBI has continued to attempt to convince policymakers of its commitment to partnership with the private sector on CI issues. For instance, in 2005 then-Director Robert Mueller III told Congress that the FBI's field offices were "developing 'business alliances' to build executive-level relationships and foster threat and vulnerability information sharing, with private industries and academic institutions located within their territories having at-risk and sensitive national security and economic technologies, research and development projects."[102] Consistent with Mueller's explanation, more than a decade later, in its 2017 budget request, the FBI indicated its continued interest in "collaboration" and "strategic partnerships" within the business and academic sectors.[103] Although the Bureau may be well-intentioned, its rhetoric should not be mistaken for reality. Policymakers assessing the counterintelligence needs of private industry should evaluate not only the FBI's statements but also its track record in this area.

Redundancy of Counterintelligence Efforts across the U.S. National Security Community

As noted above, in addition to the FBI, several other U.S. government investigative agencies field counterintelligence-oriented outreach programs. The Department of Defense, the Department of Commerce, and the Department of Homeland Security all have responsibilities in the counterintelligence field. These responsibilities appear to be at least partially redundant, and they make developing overall strategic coordination of federal efforts and allocating resources to the most important sectors and firms from a commercial counterintelligence perspective more difficult. In addition, the existence of multiple programs in different agencies can make it more difficult for the private sector to effectively work with the federal government.

The Path for Reform of Government Counterintelligence

The U.S. government has a lackluster legacy in the field of protecting the private sector and, despite recent efforts at reform, remains at a disadvantage vis-à-vis threat actors that target the U.S. private sector. As early as 2001, the NIPC was the subject of criticism by the General Accounting Office for a lack of timeliness in issuing warnings about cyberattacks. Most warnings, according to the GAO, came only once an attack was underway.[104] Furthermore, information seemed to move in only one direction. According to the CEO of the National Cyber Forensics and Training Alliance, the FBI would accept unclassified information from the private sector and then classify it, which prevented the Bureau from then sharing it with other entities in the private sector.[105]

It is not only FBI entities that have been the subject of criticism. As of 2015, DHS' US-CERT program did not provide information as quickly as private-sector cyber-analysis companies.[106] The Cybersecurity Information Sharing Act (CISA) of 2015 may do little to remedy these deficiencies. There is no guarantee that the information CISA requires to be shared will be any more timely or effectual than the underwhelming data that the private sector received prior to CISA's passage. Furthermore, CISA, even if it does prove to be successful, addresses only the cyber aspect of counterintelligence and leaves more traditional, but similarly damaging compromises (e.g., the traditional insider threat) unchecked. In a best-case scenario, CISA still does not remedy the redundancy and the fragmented implementation of counterintelligence awareness initiatives.

The Information Sharing and Analysis Centers (ISAC)s, which serve as focal points for specific economic sectors, are the closest structures that the United States currently has to platforms for leveraging private-sector expertise in furtherance of national security. The National Security Council's Richard Clarke outlined the ISAC concept in 1998 as "advanced think tanks, where the private sector could go with information and know that they could share it in a trusted agent kind of way, that it would be appropriately safeguarded and sanitized when passed on to Government agencies."[107] However, these bodies evolved into privately owned and operated entities; thus, the government is unlikely to be an equal partner. Furthermore, ISACs are not uniformly structured.[108] This may cause the ISACs' external partners confusion about how to engage these bodies, resulting in

decreased efficiency in the use of resources. Furthermore, the ISACs do not represent a complete representation of the private-sector entities at risk. According to the National Council of ISACs, these bodies are oriented around aspects of critical infrastructure.[109] This leaves some of the United States' most innovative, and consequently at-risk enterprises out in the cold. It also appears to stovepipe best-practices by sector, rather than permitting a cross-pollination of information about threats, best-practices, and lessons-learned.

From its outset, counterintelligence outreach has been a function that serves the interests of multiple U.S. government agencies—a reality that suggests the function of counterintelligence outreach should be managed as an interagency function, rather than unilaterally and duplicatively by multiple agencies. The FBI's PPP was an early example of how multiple interagency customers benefited from a parochial program. More recently, the participation of DSS in the FBI's CSP program provided an additional indicator that outreach was of interest to multiple agencies. In 2016, cyber outreach to private industry further demonstrated the redundancy of missions and capabilities across government agencies. The FBI, DHS, and DSS all issued warnings to the private sector about a cyber-espionage campaign directed at sensitive business information.[110] In the more-than-75 years of counterintelligence outreach programs, there seems to have been minimal effort to identify where efficiencies of effort could be created. Instead, one agency ends up being responsible for what should be a coordinated interagency initiative (the PPP) or, more recently, multiple agencies create redundancies by duplicating efforts.

To combat the foreign commercial intelligence threat, the U.S. government needs to refine what it expects to achieve in counterintelligence outreach.

There is also an inherent leeriness by certain elements of the private sector about working directly with a U.S. government investigative/intelligence agency. The private sector has been historically reluctant to share information—which might cause shareholders and markets to lose confidence in the firm—with law enforcement.[111] There is also a public relations consideration, which may make companies vulnerable to foreign threats. Certain firms have attempted to maintain an image of independence from the government, especially in the wake of the Snowden revelations. This was most evident in Apple's high-profile refusal to assist the FBI with unlocking the iPhone that the San Bernadino, California shooter had used. Taken to an extreme, this outlook may cause companies to shy away from appearing to proactively cooperate with authorities and only enlist the government's assistance after a loss has occurred. This not only puts companies' and shareholders' interests in jeopardy but also has the potential to harm the U.S. national interest, by inflicting economic damage and allowing adversaries to obtain proprietary intellectual property.

The Need for a New Operational Approach

To combat the foreign commercial intelligence threat, the U.S. government needs to refine what it expects to achieve from counterintelligence outreach. Private industry—because it is developing capabilities ahead of (and not at the behest of) the U.S. government—is also on the front lines in facing down foreign state, corporate and other non-state intelligence threats. Therefore, it is as likely positioned to inform the U.S. national security community about emerging threats as it is likely to benefit from U.S. government knowledge.

Counterintelligence outreach should strive not simply to guard the private sector but also to facilitate the incorporation of counterintelligence concerns into private industry's due-diligence. Although the incentive of good corporate citizenship (i.e. being security conscious for the good of the United States) is unlikely to be a salient motivator, private industry, in order to maintain the confidence of stockholders and investors, has a vested interest in preventing exploitation of its proprietary information by foreign entities. Fundamentally changing the way that industries think about the problem of counterintelligence, instead of simply providing instructions about how they can superficially change their behavior, should be the objective. The former will make private industry a true partner in counterintelligence by positioning it to understand the implications of its business decisions before they are made. This is better than simply being a client of U.S. services once threats have already taken advantage of these decisions.

Even if U.S. intelligence agencies could coordinate to reduce redundancy and maintain a consistent focus on counterintelligence outreach, their coverage of threats to private industry is incomplete. Counterintelligence is more than just catching spies who are acting illegally—it is about preventing a competitor from gaining an informational advantage. It therefore requires measures beyond what agencies such as the FBI, DHS, and DSS, which are looking strictly at activities of a criminal nature, can contribute. Missing from the current interagency approach to counterintelligence outreach is a component to assess the vulnerabilities that legal but unscrupulous activities, such as China's forcing of knowledge transfer by U.S. companies seeking to invest in the country, create.

The United States now needs to approach counterintelligence outreach as the provision of a market-oriented resource, directed at helping American companies to gain more complete information about the environment in which they are operating so that they can more effectively reduce the loss of information to competitors. Because no single government agency has an appropriately broad understanding of the issue, and because outreach serves an interagency constituency, the U.S. government should establish an interagency hub for counterintelligence outreach. This entity should be a public-private partnership, along the lines of the National Endowment for Democracy. By incorporating private-sector entities as stakeholders, rather than simply recipients of government services, this new entity would remain responsive to industry needs and concerns. The private sector is one of the new front lines in the fight against foreign intelligence—it must be able to make decisions that incorporate counterintelligence as a consideration, rather than an afterthought when something goes wrong. Because it is on the cutting edge of R&D—which draws unwanted foreign intention—it may be the first identify emerging threats. The industry-government relationship should, consequently, involve industry in defining challenges and then drawing on U.S. government agencies in response to these needs and concerns. This alleviates the need for government agencies to solely determine what works best for a milieu in which it has limited experience.

This new partnership would not engage in clandestine activities but would, instead, function as an honest broker between industry and government. One of its primary functions would be to translate sensitive concerns identified by the U.S. Intelligence Community and other collectors, into publicly distributable products and assistance. It should align these outreach efforts with industry sectors, identifying the implications of broad national security concerns for distinct subsets of customers. To provide assistance, the partnership should incorporate, deconflict, and streamline existing outreach programs (and should receive the personnel and other resources associated with those programs). Although outreach to specific commercial entities could provide an unfair advantage, the partnership should be able to connect an entity facing a specific threat with the appropriate investigative agencies. The partnership should also serve as a forum for security dialogue through which companies at risk can identify and enlist the services of private-sector cyber and other security firms, since private-sector responses have proven to be more efficient, for industry clients, than the U.S. government. A final piece—an overarching understanding of technically legal but unscrupulous foreign business practices, such as China's mercantilist approach to U.S. industry—is necessary to fully counter foreign clandestine and coercive intelligence collection activities. This could be done through resources in such a new partnership, or in close cooperation with beefed-up efforts in the National Security Council.

The U.S. government should consolidate counterintelligence outreach into a public-private partnership akin to the National Endowment for Democracy.

There is currently a window of opportunity to implement this consolidation. Dan Coats, the current Director of National Intelligence (DNI), has indicated that he is looking for opportunities to reduce the size of the U.S. intelligence community (IC).[112] In May 2017, Coats told members of the U.S. Senate that he was interested in streamlining the IC.[113] Not only would rationalizing counterintelligence awareness reduce redundancy, it would actually serve as a force-multiplier by obtaining the buy-in from private-sector entities seeking to incorporate counterintelligence into their due-diligence process in furtherance of protecting the bottom-line.

CONCLUSION

U.S. government engagement with the private sector for commercial counterintelligence is long overdue for reform. Functionally, arrangements have been inconsistent and redundant. However, even if the enterprise were running like a Swiss watch, the underlying premise is outdated. The U.S. government is no longer the driver of innovation and instead is an adopter and adapter of knowledge and capabilities developed independently of government customers. Consequently, the financial incentive for collaboration with the government has decreased. Furthermore, because the private sector is in the cross-hairs of foreign state and non-state actors, it is as likely to be able to provide insights about counterintelligence to the U.S. government as it is likely to benefit from U.S. government-imparted knowledge.

To remedy these issues, the U.S. government should consolidate counterintelligence outreach into a public-private partnership akin to the National Endowment for Democracy. Making private industry a stakeholder in such a partnership will ensure that

U.S. counterintelligence efforts respond to the needs of private industry, rather than leaving government agencies—which respond to a very different set of incentives—pondering what will appeal to private-sector customers. This partnership would absorb, deconflict, and streamline existing outreach initiatives that are currently scattered across agencies. It would also take responsibility for translating U.S. national security terms into sharable products that resonate with specific industry sectors. Finally, this hub should truly be a resource for countering foreign clandestine and coercive intelligence collection, by incorporating awareness of technically legal but unscrupulous foreign business practices that put the long-term well-being of industry (and elements of U.S. national power that rely on private sector ingenuity) in peril.

The current desire of DNI Coats to create greater efficiency within the U.S. intelligence community provides a unique window of opportunity for this project. A public-private partnership would not only consolidate currently redundant functions—by creating a single interface for counterintelligence outreach, capable of relating on industry on industry's terms—but would also free up agencies to pursue their core intelligence missions rather than engaging in prophylactic measures. After all, there is no need to divert law enforcement expertise from agencies such as the FBI and DHS to engage in non-investigative liaisons. Furthermore, a partnership would actually strengthen U.S. counterintelligence. Rather than simply changing the private sector's behavior, this new approach would help change the private sector's mindset, encouraging it to incorporate counterintelligence concerns into its due-diligence process and thereby leveraging corporate America as a force-multiplier in thwarting foreign threats to U.S. assets.

ENDNOTES

1. Robert D. Atkinson, "Testimony Before U.S. House Foreign Affairs Subcommittee on China's Threat to U.S. Advanced Industries" (Information Technology and Innovation Foundation, 2017), April 26, 2017, https://itif.org/publications/2017/04/26/testimony-us-house-foreign-affairs-subcommittee-chinas-threat-us-advanced.

2. U.S. Department of Justice, "Chinese National Pleads Guilty to Attempting to Illegally Export High-Grade Carbon Fiber to China," news release, April 21, 2017, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-attempting-illegally-export-high-grade-carbon-fiber-china.

3. U.S. Department of Justice, "Seven People Charged with Conspiring to Steal Trade Secrets for Benefit of Chinese Manufacturing Company," news release, May 24, 2017, https://www.justice.gov/usao-dc/pr/seven-people-charged-conspiring-steal-trade-secrets-benefit-chinese-manufacturing-company.

4. Ellen Nakashima, "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks," *The Washington Post*, July 8, 2017, https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html.

5. Fred Hiatt, "Soviets Shift to Commercial Spying; Primakov Says Traditional Espionage Against U.S. Has Declined," *The Washington Post*, December 13, 1991.

6. James Andrew Lewis, "The Economic Impact of Cybercrime and Cyber Espionage" (Center for Strategic and International Studies, 2013), https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage.

7. The Commission on the Theft of American Intellectual Property, *The Report of the Commission on the Theft of American Intellectual Property,* (Washington, DC: National Bureau on Asian Research, 2013), 2, http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

8. The Fourth Annual Cybersecurity Summit, held on September 25, 2013, at the National Press Club in Washington, DC (see: Joshua Philipp, "The Staggering Cost of Economic Espionage Against the US," *The Epoch Times,* October 22, 2013, https://www.theepochtimes.com/the-staggering-cost-of-economic-espionage-against-the-us_326002.html).

9. Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in An Iranian Hacking Case," *New York Times*, March 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html; Christopher M. Matthews, "Google Search Technique Aided N.Y. Dam Hacker in Iran," *The Wall Street Journal*, March 27, 2016, https://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543; James B. Comey, "Addressing the Cyber Security Threat," International Conference on Cyber Security, January 7, 2015, https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

10. Dan Steinbock, "The Challenges for America's Defense Innovation" (Information Technology and Innovation Foundation, November 2014), 15, https://itif.org/publications/2014/11/21/challenges-america%E2%80%99s-defense-innovation.

11. Anna Mulrine, "Pentagon Cybersecurity Strategy Comes with Olive Branch to Silicon Valley," *Christian Science Monitor*, April 23, 2015, https://www.csmonitor.com/World/Passcode/2015/0423/Pentagon-cybersecurity-strategy-comes-with-olive-branch-to-Silicon-Valley.

12. Josh Hicks, "Homeland Security Is Laying Roots in Silicon Valley, and You Might Not Like Its Reasons," *The Washington Post*, April 22, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/04/22/homeland-security-is-laying-roots-in-silicon-valley-and-you-might-not-like-its-reasons/.

13. Robert D. Atkinson, "Testimony Before U.S.-China Economic and Security Review Commission on Chinese Foreign Direct Investment" (Information Technology and Innovation Foundation, January 26, 2017), https://itif.org/publications/2017/01/26/testimony-us-china-economic-and-security-review-commission-chinese-foreign.

14. Thilo Hanemann and Daniel Rosen, *New Neighbors: Chinese Investment in the United States by Congressional District* (National Committee on US-China Relations and the Rhodium Group, May 2015), 60, http://rhg.com/reports/new-neighbors.

15. Robert D. Atkinson, "Testimony Before U.S. House Foreign Affairs Subcommittee on China's Threat to U.S. Advanced Industries" (Information Technology and Innovation Foundation, April 2017), https://itif.org/publications/2017/04/26/testimony-us-house-foreign-affairs-subcommittee-chinas-threat-us-advanced).

16. Joel Schechtman, Dustin Volz, and Jack Stubbs. "Under Pressure U.S. Firms Bow to Russian Demands to Share Cyber Secrets," *Reuters,* June 23, 2017, https://www.reuters.com/article/usa-russia-tech/insight-under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSL1N1JK0II.

17. Annual Report of the Attorney General of The United States, 1941. H. Doc No. 509. 77th Cong. (1940).

18. Memorandum for the Director, Federal Bureau of Investigation, November 15, 1939. Declassified July 13, 1990.

19. Raymond Batvinis, *The Origins of FBI Counterintelligence* (Lawrence, KS: University Press of Kansas, 2007) 83.

20. Memorandum for the Director, Federal Bureau of Investigation, November 15, 1939. Declassified July 13, 1990.

21. Annual Report of the Attorney General of The United States, 1941. H. Doc No. 509. 77th Cong. (1940).

22. Emergency Supplemental Appropriation Bill for 1940, Before the Subcommittee of the Committee on Appropriations House of Representatives. 76th Cong. (1939).

23. Memorandum for the Director, Federal Bureau of Investigation, August 26, 1940. Declassified July 7, 1990.

24. Ibid.

25. Memorandum for the Director, Federal Bureau of Investigation, 66-2554, November 2, 1940. Declassified July 16, 1990.

26. Ibid.

27. Memorandum for the Director, FBI Executive Conference, 66-2554. 11 April 1940,

28. The Director, Federal Bureau of Investigation, September 11, 1942, 66-2554. Declassified September 15, 1990.

29. Executive Conference to the Director, January 19, 1944. Declassified May 14, 1990.

30. Annual Report of the Attorney General of The United States, 1941. H. Doc No. 509. 77th Cong. (1940).

31. Emergency Supplemental Appropriation Bill for 1940, Before the Subcommittee of the Committee on Appropriations House of Representatives, 76th Cong. (1939).

32. Raymond Batvinis, *The Origins of FBI Counterintelligence* (Lawrence, KS: University Press of Kansas, 2007), 83.

33. Counterintelligence and National Security Information, Before a Subcommittee of the Committee on Government Operations House of Representatives. 99th Cong. (1985).

34. Ibid.

35. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism: Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?* (2014) (Statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation); Freddie L Capps Jr. "Espionage Awareness Programs," FBI Law Enforcement Bulletin, September 1991, Vol 60, No 9.

36. Douglas Jehl, "C.I.A. Nominee Wary of Budget Cuts," *New York Times*, February 3, 1993.

37. Thomas R. Stutler, "Stealing Secrets Solved: Examining the Economic Espionage Act of 1996," *FBI Law Enforcement Bulletin*, November 2000, Vol 69, No 11; *FBI Counterintelligence Visits to Libraries. Hearings before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives*, 100th Cong. 111 (1988) (Testimony of James H. Geer, Assistant Director, Intelligence Division, Federal Bureau of Investigation).

38. Gregory M. Lamb, "Leaks Flow East—and West; US Industry and High-Tech Spies," *The Christian Science Monitor*, December 28, 1982*; Hearings before the U.S. House Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary: FBI Counterintelligence Visits to Libraries,* 100th Cong. 176-177 (1988) (Testimony of James H. Geer, Assistant Director, Intelligence Division, Federal Bureau of Investigation).

39. Gregory M. Lamb, "Leaks Flow East—and West; US Industry and High-Tech Spies," *The Christian Science Monitor*, December 28, 1982.

40. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 4.

41. Freddie L Capps Jr., "Espionage Awareness Programs," *FBI Law Enforcement Bulletin*, September 1991.

42. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 6.

43. National Industrial Security Program Policy Advisory Committee Minutes of the Meeting, September 27, 1995.

44. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 7.

45. Freddie L Capps Jr., "Espionage Awareness Programs," *FBI Law Enforcement Bulletin*, September 1991.

46. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 16.

47. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 6.

48. National Counterintelligence Center, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—1995," 7.

49. "Awareness of National Security Issues and Response [ANSIR]," Federation of American Scientists, accessed August 17, 2017, https://fas.org/irp/ops/ci/ansir.htm; Thomas R. Stutler, "Stealing Secrets Solved: Examining the Economic Espionage Act of 1996," *FBI Law Enforcement Bulletin*, November 2000, Vol 69, No 11.

50. "Introduction to the Economic Espionage Act," U.S. Department of Justice, 2015, accessed September 22, 2017, https://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act.

51. John F. Lewis, Jr., "Fighting Terrorism in the 21st Century," *FBI Law Enforcement Bulletin*, March 1999.

52. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, National Counterintelligence Center.

53. John F. Lewis, Jr., "Fighting Terrorism in the 21st Century," *FBI Law Enforcement Bulletin*, March 1999.

54. "Michael J Waguespack, Deputy Assistant Director, National Security Division, FBI, before the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs and International Relations," April 03, 2001.

55. Ibid.

56. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, National Counterintelligence Center.

57. "Michael J Waguespack, Deputy Assistant Director, National Security Division, FBI, before the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs and International Relations," April 3, 2001.

58. "Economic Espionage. Protecting America's Trade Secrets," Federal Bureau of Investigation, accessed September 23, 2017, https://www.fbi.gov/file-repository/economic-espionage-1.pdf/view.

59. Darren E. Tromblay and Robert G. Spelbrink, *Securing U.S. Innovation* (Lanham, MD: Rowman & Littlefield, 2016).

60. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism: Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?* (2014)

(Statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation).

61. Ibid.

62. *Access: Official Magazine of the Defense Security Service,* Volume 2, Issue 2, Summer 2013.

63. Darren E. Tromblay and Robert G. Spelbrink. *Securing U.S. Innovation* (Lanham, MD: Rowman & Littlefield, 2016).

64. Bruce Hoffman, Edwin Meese III, and Timothy J. Roemer, *The FBI: Protecting the Homeland in the 21st Century* (9/11 Review Commission, 2015).

65. "Office of Private Sector: Executive Fact Sheet," Federal Bureau of Investigation, accessed August 27, 2017, https://www.fbi.gov/file-repository/ops-ext-508_6-10.pdf/view.

66. Ibid.

67. Darren E. Tromblay and Robert G. Spelbrink, *Securing U.S. Innovation* (Lanham, MD: Rowman & Littlefield, 2016).

68. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Cyber Attack: Improving Prevention and Prosecution,* S. Doc. 106-838, 106th Cong. (2000).

69. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Information Infrastructure Protection: The Threat Is Real,* S. Doc. 106-858, 106th Cong. (1999); *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Cyber Attack: Improving Prevention and Prosecution,* S. Doc. 106-838, 106th Cong. (2000).

70. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Information Infrastructure Protection: The Threat Is Real,* S. Doc. 106-858, 106th Cong. (1999).

71. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Infrastructure Protection: Toward a New Policy Directive,* S. Doc. 105-763, 105th Cong. (1998).

72. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Cyber Attack: Improving Prevention and Prosecution,* S. Doc. 106-838, 106th Cong. (2000).

73. Ted Bridis, "FBI Unit Fails to React on Time to Electronic Threats, Report Says," *The Wall Street Journal,* May 22, 2001.

74. Government Accountability Office, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges* (Washington, D.C.: Government Accountability Office, 2005).

75. "FBI Is Considering a Plan to Terminate Cyber-Security Unit," *The Wall Street Journal,* March 21, 2002.

76. Darren E. Tromblay and Robert G. Spelbrink, *Securing U.S. Innovation* (Lanham, MD: Rowman & Littlefield, 2016).

77. Ibid.

78. U.S. Department of Justice, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative* (Washington, D.C.: U.S. Department of Justice, 2016), 18.

79. "Office of Private Sector: Executive Fact Sheet," Federal Bureau of Investigation, accessed August 27, 2017, https://www.fbi.gov/file-repository/ops-ext-508_6-10.pdf/view.

80. Defense Security Service, "Stakeholder Report 2012," 7, http://www.dss.mil/documents/pressroom/2012-DSS-Stakeholder-Report.pdf.

81. Ibid, 11.

82. Ibid, 4.

83. "DSS Counterintelligence Partners with Industry to Mitigate Foreign Intelligence Threats," *Access: Official Magazine of the Defense Security Service,* Winter 2014; Volume 3, Issue 4.

84. U.S. Department of Commerce, Bureau of Industry and Security, "Annual Report to the Congress for Fiscal Year 2011," 13.

85. U.S. Department of Commerce, Bureau of Industry and Security, "Annual Report to the Congress for Fiscal Year 2014," 15.

86. U.S. Department of Commerce, Bureau of Industry and Security, "Annual Report to the Congress for Fiscal Year 2012," 10-11.

87. U.S. Department of Commerce, Bureau of Industry and Security, "Annual Report to the Congress for Fiscal Year 2011," 11.

88. Ibid, 13.

89. "Project Shield America," U.S. Immigration and Customs Enforcement, accessed September 22, 2017, https://www.ice.gov/project-shield-america.

90. *Hearing Before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Oversight, Investigation and Management: Homeland Security Investigations: Examining DHS's Efforts to Protect American Jobs and Secure the Homeland,* "Statement for the Record," U.S. Immigration and Customs Enforcement, July 28, 2011.

91. "Written Testimony of ICE Homeland Security Investigations Executive Associate Director Peter Edge for a Senate Committee on Appropriations Subcommittee on Homeland Security hearing titled 'Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future'," May 7, 2014, https://www.dhs.gov/news/2014/05/07/written-testimony-ice-homeland-security-investigations-senate-appropriations.

92. U.S. Department of the Treasury, "Department of the Treasury Efforts to Prevent Illicit Transfers of U.S. Military Technologies," March 23, 2000, 14, http://purl.access.gpo.gov/GPO/LPS83245.

93. U.S. Government Accountability Office, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities* (Washington, D.C.: Government Accountability Office, 2005), http://www.gao.gov/products/GAO-05-434.

94. Ibid.

95. Raymond Batvinis, *The Origins of FBI Counterintelligence* (Lawrence, KS: University Press of Kansas, 2007) 83; Annual Report of the Attorney General of The United States, 1941, H. Doc No. 509. 77th Cong. (1940).

96. FBI Oversight and Authorization, Fiscal Year 1993, Before the U.S. House of Representatives Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, 102nd Cong. (1992).

97. Ibid.

98. Oversight of the Federal Bureau of Investigation, Before the U.S. Senate Committee on the Judiciary, S. Doc 112-405, 112th Cong. December 14, 2011.

99. Jay Solomon, "FBI Sees Big Threat from Chinese Spies; Businesses Wonder," *The Wall Street Journal*, August 10, 2005, https://www.wsj.com/articles/SB112362385648509071.

100. U.S. Department of Justice, *Audit of the Federal Bureau of Investigation's Cyber Threat Prioritization* (Washington, D.C.: U.S. Department of Justice, 2016).

101. Darren E. Tromblay, "The Threat Review and Prioritization Trap: How the FBI's New Threat Review and Prioritization Process Compounds the Bureau's Oldest Problems," *Intelligence and National Security*. 31. No. 5. 2016.

102. Testimony of Robert Mueller III Before the U.S. Senate Committee on Intelligence, February 16, 2005.

103. U.S. Department of Justice, FY 2017 Authorization and Budget Request to Congress (Washington, D.C.: U.S. Department of Justice / Federal Bureau of Investigation, February 2016.)

104. Ted Bridis., "FBI Unit Fails to React on Time to Electronic Threats, Report Says," *The Wall Street Journal*. May 22, 2001.

105. U.S. Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative* (Washington, DC., U.S. Department of Justice, 2015), 20.

106. Senator Tom Coburn, *A Review of the Department of Homeland Security's Missions and Performance,* U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Cong. (Committee Print, January 2015), https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE-403C-A08A-727F89C2BC9B.

107. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Infrastructure Protection: Toward a New Policy Directive,* S. Doc. 105-763, 105th Cong. (1998). (Testimony of Richard Clarke).

108. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Information Infrastructure Protection: The Threat Is Real,* S. Doc. 106-858, 106th Cong. (Testimony of John S. Tritak).

109. National Council of ISACs, accessed September 14, 2017, https://www.nationalisacs.org

110. Joseph Cox, "You Don't See This Often: Simultaneous FBI, DHS, and DoD Cyber Espionage Alerts," *Motherboard*, May 6, 2016, https://motherboard.vice.com/en_us/article/4xa3bj/rare-simultaneous-fbi-dhs-and-dod-cyber-espionage-alerts.

111. *Hearing Before the U.S. Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information: Critical Infrastructure Protection: Toward a New Policy Directive,* S. Doc. 105-763, 105th Cong. (1998).

112. Kevin Baron, "Spy Chief Searching for Cuts across Entire US Intelligence Community," *DefenseOne,* May 11, 2017, http://www.defenseone.com/politics/2017/05/trump-searching-cuts-across-entire-us-intelligence-community/137784/.

113. Ibid.

ACKNOWLEDGMENTS

The author wishes to thank Robert D. Atkinson for providing input to this report. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Darren E. Tromblay served the U.S. Intelligence Community as an intelligence analyst for more than a decade. He is the author of The *U.S. Domestic Intelligence Enterprise: History, Development, and Operations* (Taylor & Francis, 2015) and co-author of *Securing U.S. Innovation* (Rowman & Littlefield, 2016). His forthcoming book, *Foreign Influence on U.S. Policymaking: How Adversaries and Allies Manipulate and Marginalize the American Electorate,* will be published by Rowman & Littlefield in 2018. Mr. Tromblay's work has been featured by *Lawfare, The Hill, Small Wars Journal,* and *Intelligence and National Security.* He holds an MA from the George Washington University's Elliott School of International Affairs, an MS from the National Intelligence University, and a BA from the University of California. Mr. Tromblay can be reached at Tromblay@gwu.edu. The views expressed in this essay are entirely the author's and do not represent those of any U.S. government agency or other entity.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.