Chapter published in Damien Van Puyvelde and Aaron F. Brantly, *US National Cybersecurity: International Politics, Concepts and Organization* (London and New York: Routledge, 2017)

12 From information to cybersecurity: bridging the public-private divide

Damien Van Puyvelde

In the last decade, contractors have played a significant role in the US national security effort.[1] Today, close to a million contractors hold a security clearance, which grants them access to sensitive government information.[2] The risks these cleared contractors pose to government information security have become more apparent in recent years but they have not been examined in detail. The government itself recognized in the mid-2000s that despite its efforts to maintain control over contractors, outsourcing services increase risks "by reducing control over access to systems and information".[3] In 2013, the unauthorized disclosure of sensitive government information orchestrated by former National Security Agency (NSA) contractor Edward Snowden shed light on the risks that contractors with a need to know can pose to government information security.[4] Some commentators found that the Snowden leaks exposed "cracks" in the contractor system.[5] In 2016, media reports alleged that Harold Martin, an NSA contractor working on offensive cyber warfare programs, had been taking home classified material for 16 years.[6] Recognizing these concerns, this chapter explores the risks contractors have posed to the security of sensitive government information throughout history. A particular emphasis is put on the nature of these risks, their possible evolution, and the government's efforts to mitigate them in cyberspace.

Two concepts lie at the core of this chapter: information security and cybersecurity. US law defines information security as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction."[7] Information security relies on three core components: confidentiality, integrity and availability. Confidentiality prevents sensitive information from reaching the wrong hands, integrity guarantees that information remains accurate and trustworthy, and availability ensures that only authorized parties are able to access the information. Since anything that occurs in cyberspace involves information and information systems, cybersecurity can be considered as a component of information security. There are significant overlaps between information and cybersecurity and the two terms are often used interchangeably. However, information security concerns are broader than cybersecurity concerns because they encompass the confidentiality, integrity and availability of information beyond cyberspace. For example, trusted employees can share paper copies of sensitive documents or discuss their content with outsiders. In the last decade, cybersecurity concerns have dominated public discussions about information security. This raises important questions regarding the evolving nature of compromises to national security and the need for public-private collaboration to maintain information security in cyberspace.

From a methodological point of view, the dearth of publicly available information on compromises to US national security is a significant hurdle that is worth mentioning. When compromises are made public, reports often conspicuously lack substantive detail regarding the intrusion, such as the number of systems and computers that have been compromised and the nature of the intrusion.[8] Understandably, instances and details regarding intrusions often remain unreported because of their sensitive nature, liability concerns, and the weaknesses they point

out.[9] This state of affairs complicates and limits the representativeness of research in this domain but it does not make it impossible.

The chapter first considers the historical threats and concerns relating to contractors and information security. Contractors have played a significant role in the development of the US national security effort, and as such they have benefited from and helped secure access to sensitive government information. This historical role helps explain why contractors have been involved in a series of information security breaches throughout history. However, publicly available evidence suggests that most of the compromises to US national security have originated with government employees. The fact that more government employees have accessed sensitive government information throughout the years can explain this situation.

The second section of the chapter seeks to explain compromises to US national security. Much of the discussions about compromises have focused on individual motivations to compromise national security. Yet the vulnerability of communications systems has also posed technical risks to information security. The spread of computer networks since the 1960s and the ubiquity of cyberspace in the contemporary world has increased the risk of technical vulnerabilities. The private sector has played a visible role in this context, providing a pool of expertise to the government when public officials sought new IT solutions to gather, process, store, analyze and disseminate sensitive information. Cross-sector collaboration has provided a number of opportunities for the government to augment its national security effort, but it also poses risks to national security.[10]

An examination of recent government cybersecurity breaches caused by contractors shows that the nature of compromises in cyberspace has not fundamentally changed. Individual behavior and technical vulnerabilities remain two key factors to explain compromises. However, the prominent place of the industry in cyberspace generates issues of public-private coordination, which deserve more attention as the government seeks to mitigate cyber threats. While the government has taken a series of measures to foster public-private coordination on cyber threats, further efforts are necessary to align incentives and create a climate of trust between the public and private sectors.

Contractors as historical partners and sources of compromise

The historically close bonds between the US national security apparatus and the private sector have long bred the possibility that hostile organizations could target contractors to collect sensitive government information. Throughout the nineteenth and in the first half of the twentieth century, the Pinkerton Agency provided a number of security services to the US government. Pinkerton agents conducted espionage and counterespionage for George B. McClellan, the commander of the Union's Army of the Potomac during the Civil War (1861-1865), tracked American support to Cuban rebels after the War, and helped in setting up one of the first federal criminal databases.[11] Prior to the First World War, the Pinkerton Agency also served a host of foreign governments such as Britain, France, Russia, Canada and Germany, which posed problems of reliability that discredited the company.[12] Since Pinkerton and his men served other governments to make a profit, could they be trusted with sensitive government information? The different incentives followed by government officials and private actors became increasingly

evident as the public administration paradigm emerged in the early twentieth century. The government claimed ownership over its information and Congress passed a series of laws, which made it a crime to share sensitive government information with the enemy.[13]

Concerns about national security secrets evolved with the advent of new technologies. During the Second World War, the ability of the Allies to maintain communications security and break into the communications of the Axis played a significant role in their victory.[14] In the early 1940s, Bell Laboratory provided secure teletypewriter communications systems to the US Army and Navy, and subsequently discovered the existence of compromising radio and acoustic emissions, which could have allowed the enemy to gather American secrets. Following this discovery, the laboratory developed technical counter-surveillance measures to mitigate these vulnerabilities.[15] This example shows how technical systems developed by government contractors could already create information security vulnerabilities for the government at the time.

The establishment of the US national security state in 1947,[16] and its expansion during the Cold War, provided new opportunities for the private sector to capture government contracts. As intelligence became increasingly technical, the industry provided a source of technological innovation and expertise that became essential to US national security. For instance, American companies played a crucial role in the research and development of new reconnaissance platforms such as the CORONA satellites.[17] As they expanded their contribution to the national security effort, contractors became a more visible target of infiltration.[18] As former CIA officer Robert Wallace puts it, "with more Americans working in national security disciplines having

more access, more often, to more information than ever before, the pool of potential spies is multiplied."[19]

US authorities have long been aware of the risks posed by contractors who need to know sensitive government information, and established a number of structures to liaise with the industry. In 1953, a National Security Council decision established the Communications Security Board bringing government and industry partners together to discuss and oversee communications security issues.[20] In the late 1960s, the Advanced Research Projects Agency within the Department of Defense established a taskforce to study "the risks introduced by the widespread use of resource-sharing information systems and to make recommendations to improve their security."[21] In subsequent years these recommendations were codified by various government organizations including the National Institute of Standards and Technology (NIST), a government technology agency that works with the private sector to develop standards of conduct, including information security standards. More than a decade later, a 1976 National Security Council decision expressed continuing concern about "possible damage to the national security and the economy from continuing Soviet intercept of critical non-government communications, including government defense contractors and certain other key institutions in the private sector." The decision highlighted the President's decision to extend communications security "to government defense contractors dealing in classified or sensitive information."[22]

Concerns about the ability of the private sector to maintain the security of government information were widely publicized a few years later with the release of Robert Lindsey's book *The Falcon and the Snowman: A True Story of Friendship and Espionage* and its subsequent

adaptation into a movie by John Schlesinger.[23] The fact-inspired story followed Christopher Boyce, a disillusioned employee working for an intelligence contractor, TRW, who decided to use his post in a secure communication facility to spy for the Soviet Union. When Boyce was arrested for espionage in the late 1970s, TRW became infamous for its lax security protocols.[24] This raised questions about the implementation of government-mandated information security standards in the industry. The release of the Mitrokhin archive, the collection of notes secretly made by Vasili Mitrokhin during his career as KGB archivist, confirmed that the government's concerns were justified. Documents in the archive show that the Soviet Union successfully intercepted fax communications from major defense companies working on sensitive government contracts such as Boeing, General Dynamics, Grumman, IBM, and Lockheed.[25] KGB residencies in the US also ran a series of agents who were working for leading American defense contractors such as McDonnell Douglas and TRW.[26] All these cases suggest that penetrating the US national security state through its contractors is a traditional method of infiltration used by hostile organizations.

Though US authorities have been aware of the vulnerability posed by contractors for decades, there has been little effort to systematically consider the extent of their involvement in compromises to national security. An examination of the data compiled by the Defense Personnel and Security Research Center (PERSEREC) shows that contractors have been at the origins of 10 to 15% of the publicly known compromises to national security. PERSEREC published two main reports on compromises to US national security. The first report reviews compromises to national security from 1947 to 2001 and only considers Americans as a source of compromise. In this report, 10% of the breaches originate with contractors. The second report

covers the period from 1975 to 2008 and includes both Americans and non-American sources of compromise. In this report, 15% of the compromises originate with contractors.[27] These percentages reveal the historical significance of the risk posed by contractors, but they are indicative at best. The PERSEREC databases are incomplete since they are based on publicly known compromises. More contractors have probably been involved in compromises that have remained secret or have gone unnoticed. Nevertheless, some basic conclusions can be drawn from these data. First, contractors have been involved in a significant amount of compromises to national security (at least 27 cases from 1963 to 2008). Second, the involvement of the private sector in compromises to national security has been relatively stable throughout the years, as shown in Figure 12.1. The trends shown in this figure also suggests that compromises originating with government officials have grown faster than those originating with contractors.

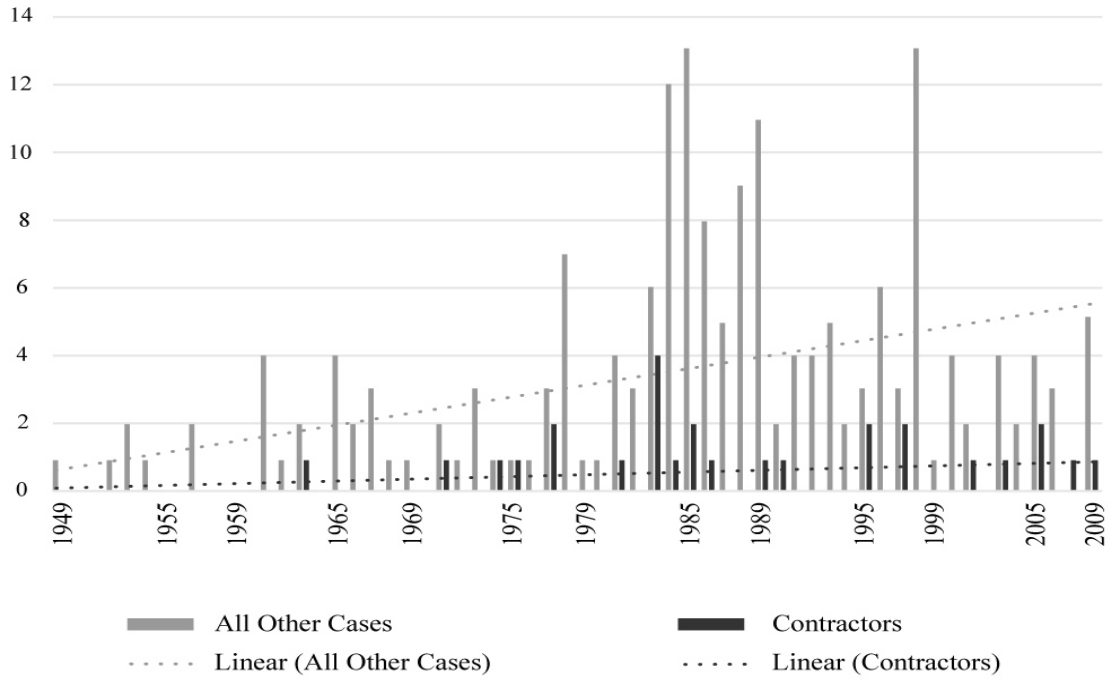

Figure 12.1 Compromises to US National Security, 1949-2008

Explaining compromises to national security

Security Studies research on compromises to national security has largely focused on insiders and their motivations to compromise the secrets of the organization they work for. Kate Randal, an insider threat analyst at the FBI, considers that information security threats are essentially "a people-centric problem" that needs to be approached in a multi-disciplinary way by combining technical, contextual, and psychosocial information.[28] Much of the research into compromises to national security, including PERSEREC reports used to develop Figure 12.1, focuses on individuals.[29] At an individual level, the psychosocial motives behind espionage and other compromises to national security are often presented thanks to the acronym MICE, which stands for money, ideology, compromise and ego. From this perspective, insiders compromise government secrets to make money, to serve an ideology, to respond to blackmail, and to satisfy their ego.[30]

The use of computer systems to process, analyze and disseminate sensitive information creates technical vulnerabilities, both at the level of the hardware and the software, that should also be taken into account in discussions about information security. Government and private sector experts started discussing these vulnerabilities publicly in the late 1960s.[31] Computer systems have provided tremendous opportunities for government and private sector organizations to improve the national security effort, for example by facilitating the processing of increasingly large numbers of logistical and operational data. However, they have also created vulnerabilities across the public-private divide.[32] As computerized networks spread throughout the 1980s, the expansion of the US national security apparatus into cyberspace provided new opportunities for

hostile actors to compromise government secrets. In 1986, Clifford Stoll, a system administrator noticed an accounting discrepancy on a computer system at Lawrence Berkeley National Laboratory. Subsequent investigations revealed that a group of West German hackers run by the KGB had penetrated sensitive systems connecting computers at Laboratory and the MITRE Corporation to access the Advanced Research Projects Agency Network/Military Network, and infiltrate dozens of computers at the Pentagon as well as at various defense contractors. The story hit the headlines when Stoll published a book recounting the story of the investigation in 1989.[33] This attack demonstrated the ability of cyber threats to spread across networks and reinforced the need for cooperation between the individuals and organizations using these networks.

In the last decades, information security threats targeting the US government and contractors' systems have become increasingly sophisticated, effective and numerous.[34] The risks posed by contractors have also become more common as the industry became a key source of IT innovation. For instance, the government has outsourced the design, implementation and maintenance of its IT systems needs to foreign countries, thus offering significant opportunities to potential adversaries to learn about US systems.[35] To be sure, the importance of individuals as sources of compromise has not disappeared in the cyber era. As a group of experts, notes all "cyber activity is ultimately the result of human motivation, behavior, and intent."[36] Foreign agents have, for example, established technology companies in the US and "served as subcontractors on U.S. defense contractors to obtain access to technology."[37] The leaks orchestrated by Edward Snowden, who used his insider position to access and disclose vast amounts of classified information, is another case in point. Snowden used his position as system administrator to access sensitive information he did not need to know, thus exposing information

security vulnerabilities in the NSA classified networks. Snowden's actions can also be explained through the lens of individual motivations. The former contractor claims his leaks served the public debate (ideological motive), but commentators have noted his actions put his ideas above the national interest (ego).[38]

The conceptual divide between insider and outsider threats can help distinguish between different types of threats that have been presented so far. Multiple rationales can explain insiders' compromise to national security, be they government officials or private contractors. Understanding the motivations driving insiders' threats to information security is important to develop appropriate countermeasures that can help identify and deter possible threats. Compromises can also be related to technical vulnerabilities originating in the public or private sector, and allowing outsiders to compromise sensitive government information. In such cases, motives matter less than the vulnerabilities that are exploited. The next section examines recent cases in which contractors compromised cyber national security to further expand this construct.

Compromises targeting contractors in cyberspace

This section examines three cases of cyber compromise that originated with contractors. These cases have been selected for convenience, because sufficient information was available about them in the public domain to illustrate some of the issues associated with contractors' information security in cyberspace.[39] In 2007, Unisys Corporation intentionally concealed a large cyber intrusion attributed to foreign hackers. The company had been contracted in 2002 by the Department of Homeland Security (DHS) to provide network and information technology

security for the Transportation Security Administration (TSA). When this initial contract ended, DHS awarded a $750 million follow-on contract to the company in 2005.[40] Unisys subsequently failed to install and manage intrusion detection systems on the TSA networks and this, some commentators note, left them vulnerable to cyberattacks.[41] From June through October 2006, Unisys experienced a security breach that occurred at an unclassified level and compromised both TSA and DHS network systems. More than 150 computers were infiltrated and unknown amounts of sensitive government information were transferred to a Chinese language website.[42] The hackers reportedly cracked the password of a network administrator at Unisys and gained access to modify system files on hundreds of computers on the DHS networks. An initial congressional investigation into the breach blamed Unisys for its negligence, and its attempt to hide security gaps and mislead DHS officials about the source of the attacks. However, the media reported that senior DHS officials also failed to recognize the situation's gravity when they were first informed of the breach.[43] The Unisys case shows how contractors can provide a gateway for hostile actors to access government networks and gather information from the outside. The possibility that Unisys concealed part of the breach from its government sponsor suggests that the incentives of the public and the private sectors were misaligned. While public authorities need to be made aware of any information security breaches to protect sensitive government information, contractors may prefer to conceal them to safeguard their reputation and maintain their competitiveness. This case highlights the need to consider organizational incentives to coordinate cybersecurity across the public-private divide.

In another case, Operation Shady RAT (an acronym for remote access tool), one single actor, widely assumed to be China, constituted an advanced persistent threat (APT) to various

international victims from mid-2006 to 2011. After gaining control of one of the servers used in this operation, the company McAfee was able to analyze and reveal its scope to the public. The attacker behind Shady RAT relied on spear-phishing techniques, the sending of e-mails with attachments to the employees of various public and private organizations. These attachments contained exploit codes that compromised the recipients' computers allowing the attacker to install software, monitor their activities and access their data. McAfee's analysis identified 71 compromised parties across a range of sectors in 14 countries. The strategy pursued by the attacker targeted both government agencies and contractors to get access to their information. At least 49 of the victims were located in the US, and included twelve defense contractors, half a dozen companies working in sensitive sectors like satellite communications, network security, information services and electronics, and a dozen government organizations at the federal, state and local levels.[44] While the details of the compromises and the specific entities that were targeted have not been disclosed, it is reasonable to assume that sensitive government information was compromised. Shady RAT shows how cyberattacks, particularly spear-phishing, can trick insiders into giving access to their computer and give hostile outsiders access to their network. In this case, insiders were apparently tricked into giving access to their computers and networks. This case is interesting because it shows how cyberattacks can rely on both technical and human vulnerabilities to compromise sensitive government information. The use of spear-phishing also suggests that human compromises are not always motivated by money, ideology, compromise or ego, but can sometimes be caused by negligence.

More recently, in June 2015, the Office of Personnel Management (OPM) revealed that a cyber intrusion within its information technology systems had compromised unencrypted databases

containing the personal information of millions of former and current federal employees. In the following month, this breach was estimated to have compromised the personal information of about 21.5 million individuals who had applied for a security clearance. This information is particularly sensitive because it contains personal information about the lives of millions of workers who have or have had access to sensitive government information. Hostile actors could use this information to identify, compromise, and recruit employees who know some of the government's secrets. The hackers behind this breach reportedly targeted an individual contractor employed through KeyPoint Government Solutions via a phishing attack to compromise his or her security credentials and gain access to OPM's systems.[45] This breach gave the attacker, widely assumed to be tied to China, access to a vast amount of sensitive information through a single entry point, thus revealing the devastating threat posed by spear-phishing and poor information security practices.[46] In October 2015, the US government began notifying OPM breach victims by providing them with identity theft services valued at a total of $133 million.[47]

These three cases show the extent of the damage that cyberattacks targeting government contractors can cause. They can also help refine the conceptual model developed above. In all three cases, a hostile actor targeted one or more individuals to gain entry into secured networks. The cases of Shady RAT and the OPM hack both relied on spear-phishing, capitalizing on the gullibility or negligence of insiders. In these two cases, no evidence suggests that the insiders had specific motivations to compromise information security. In the Unisys case, the hacker relied on external means to crack a password and infiltrate sensitive networks. The Unisys case also emphasizes issues of coordination with the private sector. This introduces an organizational

dimension, that is often overlooked in the study of compromises to national security, but crucial to the development of appropriate and timely responses to compromises.

Organizing information security across the public-private divide

The threats posed by compromises to the US government and its contractors have pushed the government to react. Since the 1990s, a long list of government strategies, reports and decisions have emphasized the need to coordinate public and private efforts to maintain information security.[48] These documents leave no doubt that government officials are well aware that contractors – which develop, operate and own a vast majority of the US critical technologies and infrastructures – need to protect their information. Federal agencies are required to protect and maintain the confidentiality, integrity and availability of their information and information systems, even when these systems are used by the private sector.[49] The government has used its authority to ensure contractors' compliance with mandated security standards. The Information Security Oversight Office, for instance, has "the authority to conduct on-site reviews of the implementation of the National Industrial Security Program by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each cooperation."[50] In 2013, the Defense Federal Acquisition Regulation Supplement was amended to include a clause requiring DoD contractors to rapidly report cyber incidents within 72 hours of discovery and communicate the extent of the compromise to the government.[51] The 2014 intelligence authorization act requires the DNI to develop procedures for intelligence contractors to report "penetrations" of intelligence community networks and information systems, give government officials access to equipment and information necessary to conduct investigations,

and establishes procedures to prohibit the dissemination of information about the breach.[52] The act also enjoined the DNI to develop security planning standards for IC networks in consultation with the industry, including a requirement that contractors develop insider threat detection capabilities. The Cybersecurity Act of 2015 mandates the establishment of procedures to facilitate timely sharing of cyber threat indicators between federal and non-federal entities. The act also provides protection from liability to the industry for the monitoring and sharing of cyber threat indicators of defensive measures.[53] This is a clear signal that the government understands the need to take into account private sector incentives to remove obstacles to cooperation.

In the last decades, the government has also established a number of forums to share information on cyber threats and coordinate cybersecurity efforts across the public-private divide but paid little attention to the private sector incentives to invest resources in these platforms. In 1998, President Clinton signed a Presidential Decision Directive encouraging the development of Information Sharing and Analysis Centers (ISAC) that could facilitate the protection of critical infrastructure and key resources through information sharing. These centers can serve as a mechanism to gather, analyze, sanitize and disseminate private sector information to the industry and the government, and for the government to share threat information with the industry.[54] The government's efforts in this domain accelerated significantly following the launch of the Comprehensive National Cybersecurity Initiative in 2008.[55] That year, the DoD established the Defense Industrial Base Collaborative Information Sharing Environment for the government to share cybersecurity products with select companies, and these companies to share anonymous intrusion reports with the DoD.[56] In 2009, representatives from NIST, the DoD and the IC set up a joint taskforce to "produce a unified information security framework for the federal

government" encompassing both national security and non-national security systems.[57] The same year, DHS opened the National Cybersecurity and Communications Integration Center (NCCIC), which brings together thirteen federal departments and agencies and sixteen private sector entities, and collaborates with over 100 private sector organizations. The center analyzes and shares information on cyber threats, and coordinates responses, mitigation and recovery efforts.[58] The NCCIC serves as the national response center during major cyber or communications incidents, helping to coordinate the efforts of multiple partners. Within the NCCIC, the Cyber Information Sharing and Collaboration Program seeks to establish a community of trust between the federal government and the critical infrastructure industry.[59] Another DHS initiative, the Enhanced Cybersecurity Services program, allows the government to share sensitive cyber threat information with accredited commercial service providers.[60] In 2015, President Obama signed an executive order to encourage companies and industries to set up Information Sharing and Analysis Organizations (ISAO). ISAOs can be used to develop a common set of voluntary standards regulating security procedures and privacy protection across the public-private divide.[61] The government has made significant efforts to raise awareness and improve public-private coordination in the field of cybersecurity, but the success of these efforts remains debated. New structures and procedures cannot guarantee public and private partners will remain committed to the improvement of information and cybersecurity.

Aligning public and private incentives

Despite the government's efforts to foster coordination across the public-private divide, problems have subsisted. Regulations requiring contractors to report cyberattacks and other

security breaches have sometimes appeared to have little effect on their behavior.[62] The reluctance of Unisys to communicate the breach it experienced in 2006 to DHS is a case in point. More recently, the Defense Security Service found that between 2009 and 2011 only 10% of cleared defense contractors reported cybersecurity breaches to their government sponsor in a given year.[63] Evidence also suggests that government contractors have underinvested in information security. In 2013, a report by the Intelligence and National Security Alliance found that a significant number of private companies working on government programs lacked a formal insider threat mitigation program.[64] The public discourse on cybersecurity has repeatedly highlighted the need for public-private partnerships and this suggests that, thus far, partnerships have remained elusive. In a recent review of national cybersecurity strategies, Madeline Carr found that public-private relations have been characterized by disjuncture about the roles, responsibility and authority of each partner.[65]

Multiple factors can explain the lack of communication between the government and the private sector. In some cases, cleared contractors may legitimately not have realized their systems came under attack. Contractors might also be aware of a compromise but prefer not to report it to government because of the absence of clear requirements or a misunderstanding of communication procedures.[66] However, given the government's regulatory and outreach efforts it is unlikely that a contractor would simply not know about its obligation to report breaches to its government sponsor. The most concerning case by far is when contractors decide not to report a compromise for fear it may impact on their reputation, benefit competitors, undermine their profit, and lead to legal pursuits.[67] In such cases, the shortfalls of cross-sector collaboration can be explained by the divergence of incentives between the government and the industry.

While companies have an interest in maintaining their security and avoiding data breaches, the need for cybersecurity can contradict their profit incentive. Maintaining demanding security standards increases costs in research and development, operations and maintenance, and administration.[68] From a business perspective, profit is more important than security. Madeline Carr notes that private sector owners accept responsibility for cybersecurity "as far as the cost of dealing with an outage promises to cost more than preventing it."[69] Companies also have an incentive to underreport or even conceal data breaches to maintain a good reputation and remain competitive. Government knowledge of their vulnerabilities could impact on their performance review and decrease their chances to get future contracts. Furthermore, the model followed by many companies is based on obtaining and selling information, not sharing it. Business incentives contrast with the government's, which is more concerned about the public interest in cybersecurity than financial and reputational costs.[70] The government's national security responsibilities create stronger incentives for public officials to seek collaboration from the industry.[71]

Most of the government's efforts to foster cross-sector collaboration on information and cybersecurity issues have relied on regulations and voluntary platforms to share information and coordinate policies. These measures are unlikely to yield significant results as long as private incentives are not aligned with the government's. If companies are not convinced that cooperating with the government and sharing sensitive information about security breaches will serve them, they will continue to seek regulatory loopholes or even disregard their obligations. This is problematic because the government needs committed private partners. With more than a

million contractors eligible for access to classified information, maintaining control over private sector uses of sensitive government information is a tremendous task.[72] The government cannot reasonably be expected to track compliance with all of its requirements and needs support from the industry.[73]

Repeated interactions are essential to improve trust between public and private partners and improve contractors' commitment to cyber national security. Scholars of social trust emphasize the importance of "shared identity and solidarity, such as common values, group membership, and the feeling of working towards common goals," in building trust.[74] This approach is in line with discussion about public-private partnerships, which have become a mainstay of the public discourse on cybersecurity.[75] Partnerships suppose a high level of trust corresponding to a mutual belief in the positive gains of collaboration. Focusing on the development of social capital, in addition to external guarantees to cooperative behavior such as regulatory requirements, has the potential to reorient private sector calculations and improve partnerships.[76] In the Netherlands, for example, cross-sector collaboration on cybersecurity has developed through the organization of periodic conferences where public and private actors sit down together and discuss the challenges they confront.[77] Events like the White House Summit on Cybersecurity and Consumer Protection of 2015 provide multiple opportunities for public and private sector leaders to engage in formal and informal forms of dialogue. These interactions should not be limited to senior executives, but also involve mid- and entry-level professionals. Multiplying opportunities for shared training and education is another way to foster cross-sector interactions while improving cybersecurity skills across the board.[78] Education also provides opportunities to disseminate the latest knowledge and drive collaboration through evidence. Recent research conducted by the

Ponemon Institute, for instance, shows that sharing threat intelligence could thwart 39 percent of cyberattacks.[79] Over the long term, dialogue and interactions have the potential to foster a culture of collaboration that is essential to protect the nation's information systems.

Conclusion

This chapter has explored issues of information and cybersecurity across the public-private divide. The long history of cross-sector collaboration on sensitive national security programs has made the private sector a constant source of compromise. The chapter reviewed a series of compromises originating with contractors to better understand their sources, and concluded that compromises are not fundamentally different across the public-private divide. Individuals, whether they are government officials or contractors, sometimes decide to leak sensitive government information. In such cases, money, ideology, compromise and ego best explain their behavior. They can also inadvertently give access to sensitive information, for example when they fall victim to a spear-phishing scam. Technical vulnerabilities can also allow external actors to infiltrate government systems and gain access to sensitive information. As the government shares sensitive information with its contractors, it needs to coordinate its efforts to mitigate these threats with the private sector. This organizational dimension has become increasingly important in the last decades and the government passed a number of laws and regulations to require and foster information sharing with its private partners. However, effective cross-sector collaboration cannot be forced onto the industry. The social dimension of public-private partnerships is equally important. Frequent interactions and shared training have the potential to

develop a culture of collaboration that will improve information and cybersecurity across the public-private divide.

Notes

[1] See for example: Peter W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (New York: Cornell University Press, 2003); Deborah Avant, *The Market for Force. The Consequences of Privatizing Security* (Cambridge: Cambridge University Press, 2005); Glenn Voelz, "Contractors and Intelligence: The Private Sector in the Intelligence Community," *International Journal of Intelligence and CounterIntelligence* 22/4 (2007): 588-91; Tim Shorrock, *Spies For Hire. The Secret World of Intelligence Outsourcing* (New York: Simon and Schuster, 2008).
[2] Office of the Director of National Intelligence, National Counterintelligence and Security Center, 2015 Report on Security Clearance Determinations, June 28, 2016, 5.
[3] National Science and Technology Council, Federal Plan for Cyber Security and Information Assurance Research and Development, Report by the Interagency Working Group on Cyber Security and Information Assurance, April 2006, 8; Government Accountability Office, Information Security: Improving Oversight of Access to Federal systems and Data by Contractors Can Reduce Risk, Report to Congressional Requesters, April 2005, 2; Government Accountability Office, Information Security. Weaknesses Continue Amid New Federal Efforts to Implement Requirements, October 2011, 32.
[4] Kimberly Dozier and Stephen Braun, "Edward Snowden Leaks Lead To Pentagon Change, Top Official Says," *Huffington Post*, February 4, 2014.
[5] Philip Ewing and Tony Romm, "Edward Snowden leak exposes cracks in contractor system," *Politico,* June 9, 2013, at http://www.politico.com/story/2013/06/edward-snowden-leak-contractor-92472_Page2.html.
[6] Scott Shane, Matt Apuzzo and Jo Becker, "Hacking Tools Among Data Stolen From U.S.," *New York Times*, October 20, 2016, A1.
[7] US Code, Chapter 44, § 3542 – Definitions (2016).
[8] Dmitri Alperovitch, Revealed: Operation Shady RAT Version 1.1, 2011, 2.
[9] John Esterbrook, "Many Hack Attacks Go Unreported," *CBS News,* April 7, 2002 at http://www.cbsnews.com/news/many-hack-attacks-go-unreported/.
[10] Barry M. Leiner et al., "The Past and Future History of the Internet," *Communications of the ACM* 40/2 (1997): 102-108; Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007); Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (London: Penguin, 2011).
[11] Frank Morn, *The Eye That Never Sleeps: A History of the Pinkerton National Detective Agency* (Bloomington, IN: Indiana University Press, 1982), 63; James MacKay, *Allan Pinkerton: the Eye Who Never Slept* (Edinburgh: Mainstream Publishing Company, 1996), 11, 71-2, 78,

149-53, 183; Bruce Durie (ed.), *The Pinkerton casebook* (Edinburgh: Mercat Press, 2007), 1, 36, 176

[12] Rhodri Jeffrey-Jones, *American espionage* (New York: The Free Press, 1977), 3, 16-21, 26 37, 55.

[13] US Congress, Defense Secret Act, 62nd Congress, 1st sess., March 3, 1911; idem, Espionage Act, 65th Congress, 1st sess., June 15, 1917; idem, Sedition Act, 65th Congress, 2nd sess., May 16, 1918.

[14] Harry Hinsley, *British Intelligence in the Second World War. Abridged version* (New York: Cambridge University Press, 1993).

[15] National Security Agency, "TEMPEST: A Signal Problem," *Cryptologic Spectrum* 2/3 (1972): 27.

[16] US Congress, National Security Act, 80th Congress, 1st sess., July 26, 1947, Titles I and II.

[17] Kevin C. Ruffner, CORONA: America's First Satellite Program (Washington D.C.: Center for the Study of Intelligence, 1995), 37.

[18] Matthew M. Aid, "All Glory is Fleeting: Sigint and the Fight Against International Terrorism," *Intelligence and National Security* 18/4 (2003): 72-120; Ayse Ceyhan, "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics," *Surveillance & Society* 5/2 (2008): 102-23.

[19] Robert Wallace, "A Time for Counterespionage," in Jennifer E. Sims and Burton Gerber (eds), *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence* (Washington: Georgetown University Press, 2009), 115.

[20] National Security Council, Decision 168, Communications Security, October 20, 1953.

[21] Evan E. Anderson and Joobin Choobineh, "Enterprise information security strategies," *Computers & Security* 27 (2008): 23; Willis H. Ware, Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, RAND Report R-609-1, Reissued October 1979, xi.

[22] Brent Scowcroft, National Security Council, National Security Decision Memorandum 338, Further Improvements In Telecommunications Security (TS), September 1, 1976, 1.

[23] Robert Lindsey, *The Falcon and the Snowman: a true story of friendship and espionage* (New York: Simon and Schuster, 1979); Gabriel Katzka and John Schlesinger (Producers), John Schlesinger (Director), *The Falcon & the Snowman* (1985).

[24] Michael J. Sulick, *American Spies. Espionage against the United States from the Cold War to the Present* (Washington D.C.: Georgetown University Press, 2013), 62-3.

[25] Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive. The KGB in Europe and the West* (London: Allen Lane, 1999), 454.

[26] Ibid, 280-81.

[27] Katherine L. Herbig and Martin F. Wiskoff, Espionage Against the United States by American Citizens 1947-2001, Technical Report 02-5, July 2002; Defense Personnel Security Research Center, Espionage and Other Compromises to National Security 1975-2008, November 2, 2009.

[28] Editor, "RSA 2013: FBI offers lessons learned on insider threat detection," at http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.

[29] Theodore R. Sarbin, "Computer Crime: A Peopleware Problem," Proceedings of a Conference held 26-26 October 1993; Center for the Study of Intelligence, *Of Moles and Molehunters: A Review of Counterintelligence Literature, 1977-92*, October 1993; Frank J. Rafalko (ed.) *A Counterintelligence Reader: American Revolution into the New Millenium, Volume Four* (Washington, DC: National Counterintelligence Center, 2004); Stephen R. Band et al., Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, December 2006, vii, 4.
[30] Stan A. Taylor and Daniel Snow, "Cold war spies: Why they spied and how they got caught," *Intelligence and National Security* 12/2 (1997): 101-125; Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS," *Studies in Intelligence* 57/1 (2013): 7-17.
[31] Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27/5 (2012): 783-5.
[32] Corey D. Schou and Kenneth J. Trimmer, "Information Assurance and Security," *Journal of Organizational and End User Computing* 16/3 (2004): ii; Intelligence and National Security Alliance, Cyber Intelligence. Setting the landscape for an emerging discipline, September 2011, 7; Evan E. Anderson and Joobin Choobineh, "Enterprise information security strategies," *Computers & Security* 27 (2008): 22.
[33] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionnage* (New York: Simon & Schuster, 1989); Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and CounterIntelligence* 6/4 (1993): 415-18.
[34] Government Accountability Office, Information Assurance. National Partnership Offers Benefits, but Faces Considerable Challenges, Report to the Honorable William Lacy clay, House of Representatives, March 2006, 1. On the rising number of cyber threats, see: Department of Homeland Security, US-CERT Year in Review. United States Computer Emergency Readiness Team, CY 2012, 6; Verizon, 2014 Data Breach Investigations Report, 38.
[35] Intelligence and National Security Alliance, Cyber Intelligence. Setting the landscape for an emerging discipline, September 2011, 6.
[36] Intelligence and National Security Alliance, Operational Cyber Intelligence, October 2014, 5.
[37] National Science and Technology Council, Federal Plan for Cyber Security and Information Assurance Research and Development, Report by the Interagency Working Group on Cyber Security and Information Assurance, April 2006, 8-9.
[38] On the Snowden affair, see: Loch K. Johnson et. al, An *INS* Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security* 29/6 (2014): 793-810; US House of Representatives, (U) Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, September 15, 2016.
[39] One case, in which a Department of Defense contractor was compromised of 24,000 files, was left aside because of the paucity of publicly available information. For more information see: Thom Shanker and Elisabeth Bumiller, "After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action," *New York Times*, July 14, 2011, A6; Jeremy White, "Government Hacked: 24,000 Files Stolen in Worst Pentagon Cyber Attack," *International Business Times*, July 14, 2011.

[40] Robert Block, "Unisys Denies Coverup of Security Breaches," *Wall Street Journal*, September 25, 2007, A15.
[41] Jason Mick, "Unysis Blamed for China-Connected Homeland Security Hacks," *DailyTech*, September 26, 2007, at http://www.dailytech.com/Unisys+Blamed+for+ChinaConnected+Homeland+Security+Hacks/article9043.htm.
[42] Block, "Unisys Denies Coverup of Security Breaches."
[43] Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *Washington Post*, September 24, 2007, A1.
[44] Alperovitch, *Revealed: Operation Shady RAT Version 1.1*, 3-9.
[45] Kristin Finklea et al., Cyber Intrusion into U.S. Office of Personnel Management: in Brief, Congressional Research Service Report, July 17, 2015, 1.
[46] Brendan, I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016.
[47] Joe Davidson, "Months after government hack, 21.5 million people are formally being advised, and offered help," *Washington Post*, October 2, 2015, A19.
[48] White House, Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998; idem, Defending America's Cyberspace. National Plan for Information Systems Protection, 2000; General Accounting Office, Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies, September 6, 2000; White House, Executive Order 13231. Critical Infrastructure in the Information Age, October 16, 2001; General Accounting Office, Critical Infrastructure Protection. Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems, July 2002, 20-1; White House, National Strategy to Secure Cyberspace, February 2003, ix; Government Accountability Office, Industrial Security. DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient, July 15, 2005, 1; White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, January 9, 2008, 7; idem, Cyberspace Policy Review, May 8, 2009; idem; Presidential Policy Directive 8 on National Preparedness, March 30, 2011; idem, Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.
[49] Government Accountability Office, Information Security. Weaknesses Continue Amid New Federal Efforts to Implement Requirements, 38; US Congress, Federal Information Security Management Act (FISMA), 107th Congress, 2nd sess., December 17, 2002; Federal Acquisition Regulation 52.239-1, Privacy or Security Safeguards.
[50] White House, Executive Order 12829, January 6, 1993.
[51] Department of Defense, Defense Federal Acquisition Regulation Supplement. Clause 252.204-7012. Safeguarding Unclassified Controlled Technical Information, November 18, 2013.
[52] US Congress, Intelligence Authorization Act for Fiscal Year 2014, 113th Congress, 2nd sess., June 11, 2014, Sec. 325.
[53] US Congress, Consolidated Appropriations Act, 2016, Division N-Cybersecurity Act of 2016, 114th Congress, 1st sess., December 15, 2015.
[54] White House, Presidential Decision Directive/NSC-63.

[55] White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23*, January 8, 2008.
[56] Thomas, "Securing Cyberspace Through Public-Private Partnership, 24.
[57] Government Accountability Office, Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems, Report to the Chairwoman, Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives, GAO-10-916, September 2010, 13.
[58] National Cybersecurity and Communications Integration Center, at https://www.dhs.gov/national-cybersecurity-and-communications-integration-center; Intelligence and National Security Alliance, Strategic Cyber Intelligence, March 2014, 6
[59] Department of Homeland Security, "Cyber Information Sharing and Collaboration Program (CISCP)," at <https://www.dhs.gov/ciscp>.
[60] Department of Homeland Security, "Enhanced Cybersecurity Services (ECS)," at <https://www.dhs.gov/enhanced-cybersecurity-services>; Scott E. Jasper, "U.S. Cyber Threat Intelligence Sharing Frameworks," *International Journal of Intelligence and CounterIntelligence* 30/1 (2017): 59.
[61] Executive Office of the President, Executive Order Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015.
[62] White House, Executive Order 12829 - Intelligence and National Security Alliance, A preliminary examination of insider threat programs in the U.S. private sector, September 2013, 8.
[63] Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011, A-1.
[64] Intelligence and National Security Alliance, A preliminary examination of insider threat programs in the U.S. private sector, 1,5.
[65] Madeline Carr, "Public-private partnerships in national cyber-security strategies," *International Affairs* 92/1 (2016): 44.
[66] US Senate, Committee on Armed Services, Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors, 113th Congress, 2nd sess., September 17, 2014, 17-20.
[67] Shorrock, *Spies for Hire*, 309, 323; Government Accountability Office, Critical Infrastructure Protection: Key Private and Public Cyber Expectations need to be Consistently Addressed, July 15, 2010, 22.
[68] J. Todd Hamill, Richard F. Deckro, Jack M. Kloeber Jr., "Evaluating information assurance strategies," *Decision Support systems* 39 (2005): 464; Anderson and Choobineh, "Enterprise information security strategies," 23.
[69] Carr, "Public-private partnerships in national cyber-security strategies," 57.
[70] Ibid, 55.
[71] Daniel Javorsek II et al., "A Formal Risk-Effectiveness Analysis Proposal for the Compartmentalized Intelligence Security Structure," *International Journal of Intelligence and CounterIntelligence* 28/4 (2015): 736.

[72] Secrecy News, Security-Cleared Population Rises to 5.1 Million, 24 March 2014, at http://fas.org/2014/03/security-cleared; Office of the Director of National Intelligence, 2013 Report on Security Clearance Determinations, 4.
[73] See for example: Government Accountability Office, Industrial Security. DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient, Report to the Committee on Armed Services, US Senate, July 2005; Government Accountability Office, Information Security. Weaknesses Continue Amid New Federal Efforts to Implement Requirements, 32; White House, Office of Management and Budget, Suitability and Security Processes Review Report to the President, February 2014, 4.
[74] Vincent Charles Keating and Erla Thrandardottir, "NGOs, trust, and the accountability agenda," *The British Journal of Politics and International Relations* (online 2016): 7-8.
[75] See for example: White House, Office of the Press Secretary, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," February 13, 2015.
[76] Keating and Thrandardottir, "NGOs, trust, and the accountability agenda," 10
[77] Max Manley, "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership," *Journal of Strategic Security* 8/3 (2015): 94.
[78] W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale and Don Welch, "A Model for Information Assurance: An Integrated Approach," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, US Military Academy, West Point, June 5-6, 2001, 30; Manley, "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership," 85.
[79] Ponemon Institute, "Flipping the Economics of Attacks," January 26, 2016.