Outsourcing in Intelligence and Defense Agencies: A Risk of an Increase in the Proliferation of Cyber Weapons?

Omree Wechsler

The many cases of the leakage of classified materials belonging to intelligence and defense agencies have led to claims that contract workers are the reason for these incidents, due to either their lack of loyalty or negligence. In addition, these leaks of classified information, including hacking programs and components, have raised the question of whether this internal threat is also the cause of the increased proliferation of sophisticated cyber weapons among players who do not have the ability to develop them. A prominent case study from the past few years is the leak of the National Security Agency (NSA)'s hacking component, EternalBlue, and its use in the global cyberattack WannaCry, which damaged computers in 150 countries and was attributed to North Korea. Understanding the internal threat and its connection to the proliferation of cyber weapons, along with enumerating the advantages and disadvantages of hiring contractors, is critical for minimizing the threat, coping with it, and in preventing harm to national security and further deterioration of stability in cyberspace.

Keywords: Outsourcing, proliferation of cyber weapons, intelligence, contractors, information security

Omree Wechsler is head of Cyber Research at the Yuval Ne'eman Workshop for Science, Technology, and Security and at the Blavatnik Inter-Disciplinary Cyber Research Center at Tel Aviv University.

Introduction

Much has been said about the disadvantages of outsourcing and privatizing of non-cybernetic security functions and services, which include problems of ethics and accountability when transferring the authority to use force into the hands of private companies. A number of leaks of classified materials, some of which have included source code of hacking tools, have led US senior officials to express the dangers of hiring contract workers in sensitive security industries, including the cyber industry.

After the Vault 7 leak, which included source codes of a CIA hacking tools, Director of the CIA and American Defense Secretary Leon Panetta said that employing contract workers carried risks, and that it was possible that they did not have the same loyalty to the organization that the agency's permanent employees had.[1] After another leak, Republican Senator Ben Sasse claimed that the NSA had to solve the problem of the leaks, the source of which was the agency's contractors.[2] These statements suggest that contract employees at American intelligence agencies are considered more problematic than permanent government employees.

The use of contractors—who are neither part of the regular army nor members of government or administration—for the purpose of carrying out warfare or espionage missions is not new and developed in historical times. The phenomenon of outsourcing for warfare, intelligence gathering, logistics, weapons development, security and consulting has been the norm throughout global military history and is becoming more widespread today. The Iraq War (2003) is one example, in which some 200,000 contract workers from private companies were deployed alongside 165,000 American soldiers.[3]

The phenomenon of outsourcing has also spread to the cyber field, especially as governments started using cyber for warfare and intelligence gathering. The two main reasons for outsourcing in intelligence gathering, cyber weapons development, and carrying out cyber operations are attributed to cutbacks in personnel and budgets and to quick technological developments in the field of information and communications technologies in the civilian

[1] Andrea Mitchell and Ken Dilanian, "WikiLeaks Release already Damaging U.S. Intelligence Efforts," *NBC News*, March 10, 2017, https://nbcnews.to/2JTpPkR.

[2] Eric Geller and Cory Bennet, "NSA Contractors Back in Spotlight after Reported Russian Theft," *Politico*, May 10, 2017, https://politi.co/2ERp7jI.

[3] Alan Axelrod, *Mercenaries: A Guide to Private Armies and Private Military Companies* (Thousand Oaks, CA: CQ Press, 2014), pp. 3–8.

sector, which has provided the private market with a clear technological advantage over governments.

Outsourcing in both the fields of intelligence and offensive cyber capabilities occur on several levels. In many cases, research and development functions have been privatized in order to receive access to advanced technology and to quickly develop weapons. In other cases, cyber operations are being privatized because privatization provides governments with plausible deniability and the ability to absolve themselves of responsibility the moment the source of the attack is identified and thus avoid public relations damage or retaliation. It is important to distinguish between the outsourcing of cyber warfare and operations and the privatization in Western countries that includes support operations, such as research, development, and information gathering and processing.

In recent years, the theft of hacking tools, malware and spyware from the computers of intelligence agencies and cyber agencies' internal employees or contractors, along with discussions and statements about the role of the contractors, demonstrate the potential risk in privatizing support activities for operations. Examples from the physical world also indicate that the trend of privatization in the cyber field could spill over into other activities, such as carrying out offensive operations in cyberspace, even among Western governments.

The basic premise of this article is that there is a connection between the phenomenon of outsourcing and an increase in the proliferation of sophisticated cyber weapons. The article suggests ways to handle the risk and to minimize its consequences. Specifically, this article focuses on leaks over the past few years of hacking programs and cyber weapons, which could be the reason for the increase in the proliferation of these weapons, and examines whether these leaks can be connected to contractors. The article examines whether programs or codes have been stolen, sold without approval or leaked, and whether they could be used afterwards for attacks. In addition, this article looks at incidents of negligence in which there was the potential for the theft or leak of components that could be used for attacks. Leaks of cyber weapons, whether malicious or as a result of negligence, can create a situation in which states lacking resources or high level technological capabilities, terrorist organizations, or criminals—can repurpose malware and thus equip themselves with advanced capabilities that they did not previously have.[4] Therefore, the proliferation of cyber weapons is defined here as the sale by unauthorized bodies, theft, or leak of hacking components, information on zero-day vulnerabilities, and malicious codes, which could potentially reach or already has fallen into the hands of others.

The article explains the phenomenon of outsourcing within the US intelligence and cyber community, as well as its advantages and disadvantages. The aim of the article is not to rule out outsourcing, as it turns out that also systems operated by permanent government employees are being hacked, enabling the theft or leak of cyber weapons or classified materials also from organizations that belong to the government. The article also seeks to increase awareness of the need for increased government supervision and for placing responsibility and accountability on government bodies or private companies that work for governments. Supervising, maintaining procedures, bestowing responsibility, and applying regulation, along with technological aids, can help government bodies supervise contract workers. Economic incentives can also help contractors improve their cyber security and encourage them to provide their employees with training on cyber hygiene and better supervise their work.

Outsourcing and Privatization of Intelligence and Cyber Services—A Theoretical Framework

This section suggests a theoretical framework for outsourcing the functions and activities that are reserved for cyber and intelligence agencies. It is important to note that outsourcing varies by country and is generally dependent on the historical context and organizational culture. However, outsourcing has a number of inherent advantages and disadvantages that should be discussed.

Why Do Governments Privatize Intelligence and Cyber Services?

Budget and personnel

Outsourcing is a practice that aims, first and foremost, to increase the efficiency of an organization and to save costs. The incentive to take activities outside of the organization and transfer them to external companies or workers is

[4] Daniel Cohen and Aviv Rotbart, “The Proliferation of Weapons in Cyberspace,” *Military and Strategic Affairs* 5, no. 1 (April 2013): 49.

based on the idea that organizations are unable to optimally perform all their activities; thus, in order to increase their competitive advantage, they must focus on their core activities and on those at which they excel and transfer all non-core activities to external companies.[5]

This theory of outsourcing is also relevant to the field of intelligence and cyber. Since intelligence agencies do not need to maintain a competitive advantage in the market, outsourcing serves mainly to reduce costs and streamline the organization. In terms of the development of cyber weapons, privatization has become a way of coping with budget cuts and personnel shortages in intelligence agencies. It should be noted that the problem of personnel shortages could result not only from budget cuts, but also from personnel restrictions and quotas that are imposed on intelligence agencies by supervisory bodies, and/or the departure of skilled personnel for the private market. Budget cuts in resources and/or personnel force intelligence agencies to employ fewer internal personnel, and as a result, they are unable to offer high salaries in order to attract talented and skilled personnel. This situation leads to the establishment of private companies that can offer better employment conditions, and thus recruit high-quality personnel.

An example of needing to cope with budget and personnel cuts can be seen at the end of the Cold War. The fall of the Soviet Bloc led to the dissolution of the main adversary of the United States, around which its massive intelligence apparatus had been built over several decades. As a result, the intelligence agencies faced extensive budget cuts and were forced to fire many employees and send others to early retirement. The cuts to the budgets and personnel of US intelligence agencies during the years 1990–1995 amounted to 16 percent of the budget and 20 percent of the personnel of the entire intelligence community. Among the intelligence agencies, the NSA suffered the most significant cutbacks: around a third of the agency's budget was cut during these years, leading to a similar cut in its labor force. Despite these changes, the US intelligence agencies quickly faced new challenges and a range of new global threats, including concerns about the security of nuclear weapons in the new post-Soviet states, along with drug trade, organized crime, terrorism, and ethno-political conflicts.

[5] Ian McCarthy and Angela Anagnostou, "The Impact of Outsourcing on the Transaction Costs and the Boundaries of Manufacturing," *International Journal of Production Economics* 88 (2004): 62.

Surge capacity

Outsourcing is also an efficient practice for dealing with a possible discrepancy between the force structure of intelligence agencies—and later among cyber agencies within the defense apparatus—and the operational requirements relating to the number of targets or threats. Outsourcing enables flexibility and the ability to allocate skilled personnel and resources in order to cover a large number of threats simultaneously as needed.[6] Flexibility is necessary as a result of the development of the threat environment to national security and the appearance of different scenarios deviating from the focus on conflicts between countries, such as terrorism, the proliferation of weapons of mass destruction, international criminal organizations, genocide, ethnic conflicts, and, in more recent years, the cyber threat.[7] The need for flexibility also applies in the cyber age as new products on the market, such as operating systems, mobile phones, and apps, require focusing on the discovery and research of security vulnerabilities and the development of exploits.

Rapid pace of technological advancements

The rapid pace of change in communications and information technology is another factor that provides a significant advantage to the private market's analysis and processing capabilities. From the 1970s until the early 1990s, intelligence agencies believed that governments had the best access to R&D of advanced technologies and of information gathering and analysis systems. This belief eroded as information became cheaper and more readily available.[8]

The connection and the increasing access to the internet since the 1990s led to sharp and exponential growth in the number of users using networks for the purpose of interactions and exchanges of information, cooperation, and more. These changes apply not only to computers but also to all electronic devices that communicate with other devices, such as satellites, command and control systems, and so forth. The appearance of technologies, such as cell phones and satellite communication, advanced sensors, powerful processors, and encryption programs, provided the private market with a

[6] Glenn James Voelz, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations* (Joint Military Intelligence College, 2016), p. 2.

[7] Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age* (New Haven and London: Yale University Press, 2010), pp. 51, 56.

[8] Ibid, p. 23.

significant technological advantage over legacy systems that are sometimes still used by government, military, and intelligence bodies.

These changes also led to behavioral and cultural changes related to the handling of accessible and readily available information. In the past, information was a rare and valuable resource and considered the province of intelligence agencies; the information and technology revolution, however, made information and data more readily available. The competitive mechanisms of the private market, according to which technological companies develop new products and technologies and launch them at a fast pace, provides this market with an almost constant advantage.[9] In addition, the private market responds better to technological developments and changes, enabling quicker responses and the provision of superior services. This is even more so when it comes to exploiting information technologies. Under these conditions, the challenge of the intelligence agencies does not relate to whether they should turn to the private market to receive access to advanced technology, new services, and research and development but rather how they should exploit the advantages of the private market for security needs.

In the American case, we can point to technological developments in the field of information and communications technologies and the transitions in countries such as Libya, Iraq, Syria, Iran, and North Korea that have moved from using radio circuits to using communications infrastructure buried underground and optical fibers. These changes have posed a challenge to the SIGINT capabilities of US intelligence and have required it to constantly invest in technology.[10]

Difficulties in attributing cyberattacks

One of the well-known challenges of cyber warfare and one of its great advantages for the attackers is the difficulty in attributing cyberattacks. Unlike kinetic attacks, in cyberspace it is difficult to trace and identify the source of the attack. Even when the computer that carried out the attack is discovered, there can be no assurance as to whether it belongs to the assailant, or whether it has in itself been hacked and used for the purpose of the attack without the knowledge of its owner. In addition, hackers have many tools

[9] Ibid, pp. 18–23.

[10] Matthew Aid, *The Secret Sentry* (New York: Bloomsbury, 2010), pp. 196–198.

that enable them to cover or erase their tracks, to mislead investigators, and to destroy evidence.[11]

Transferring the execution of offensive cyber operations to private hands makes it even more difficult to attribute the attack, as even if the attacked party succeeds in tracing the assailants, it will have to prove that a government was behind the attack. Thus, transferring offensive cyber operations to private hands can provide governments with plausible deniability and minimize the chance of a response from the attacked state.

Exporting activities that do not comply with a country's laws or constitution
Exporting activities to develop hacking tools and executing offensive cyber operations can raise questions about the accountability and oversight when these activities are authorized and approved by the government but are conducted beyond the jurisdiction and supervision of formal supervision and review bodies, such as parliamentary committees and regulatory bodies. As third parties, private companies that carry out offensive cyber operations and espionage for intelligence agencies are not subject to the regulatory bodies nor to the supervision that could delay or prevent operations, which are seen as essential and whose secrecy and speed of execution are vital for achieving their objective. This aspect, which has both advantages and disadvantages, previously has been discussed in the context of interrogating terrorism suspects but becomes even more significant when related to the need to exploit breaches and vulnerabilities in order to hack into computers and networks as part of an active defense operation, counter-espionage, or to prevent terrorist attacks.

The Risks and Disadvantages of Outsourcing in Cyber and Intelligence Fields

The phenomenon of outsourcing in cyber and intelligence fields involves also risks and disadvantages. Some of these risks and disadvantages have been discussed in the contexts of outsourcing in the fields of physical warfare, interrogations, and assistance in targeted killing operations. Cyberspace, in particular, is a relatively new area of warfare, uniquely characterized by an extensive attack surface; a wide spectrum of attackers with different

[11] Bruce Schneier, "Attack Attribution in Cyberspace," *Schneier on Security*, January 8, 2015, https://www.schneier.com/blog/archives/2015/01/attack_attribut.html.

backgrounds and interests, including civilians such as criminals or companies; an absence of physical distance and of physical borders; and a lack of clear definitions of what is legal and what is not. These characteristics of cyber, together with the risks and disadvantages of outsourcing in the fields of security, military, and warfare, render outsourcing risky for civilians, companies, government bodies, and organizations, which are far from the battlefield and are not involved in warfare. Another risk inherent in outsourcing is that operations dependent upon security clearance can be subjected to misuse and corruption.

Competition between the private market and intelligence agencies

Outsourcing has led to the creation of a private market for government activities. The growth of this market creates the effect of an infinite loop: The outsourcing of an increasing number of governmental functions leads to the growth of the private market and increases the salaries it offers. This places government organizations, including intelligence agencies, in competition with the private market, which attracts employees from these organizations and all talented workers available in the market.

The high salaries and better benefits offered by the private market also lead to the phenomenon of a "revolving door," known in the United States also as "bidding back," in which government employees leave for the private market and return to work for government agencies as private consultants at higher salaries. This phenomenon creates a flow of cyber and intelligence agency employees into the private market, thus causing a brain drain that exacerbates the government personnel problem, which they had tried to solve through outsourcing in the first place.[12]

In particular, the American private market grew sharply in the 2000s following the burst of the dot-com bubble,[13] which created a reservoir of personnel for defense agencies. Several companies, established by former members of the defense and intelligence agencies, hired the services of analysts

[12] Patrick Radden Keefe, "Don't Privatize Our Spies," *New York Times*, June 25, 2007, https://www.nytimes.com/2007/06/25/opinion/25keefe.html.

[13] The dot-com was an economic bubble that grew in 1997–2001, when many internet companies were established as businesses and customers alike adopted the internet, together with the fast growth of stock prices, speculation on their value, and the availability of investment money. With the bursting of the bubble, many internet companies became obsolete and closed.

and former military and intelligence personnel and created divisions and departments that initially engaged in intelligence and later in cyber activities. These companies were the only ones whose employees had both sufficient experience and security clearance. The major defense contractors, such as Boeing, Lockheed Martin, and Northrop Grumman, also created departments that deal with cyber and the development of hacking components.

Figures on the total extent of outsourcing in the fields of intelligence and cyber are classified information, which makes it difficult to properly study the scope of the phenomenon. However, figures from 2007 pointed out that around 70 percent of the US intelligence budget was allocated to private companies.[14] According to rough estimates given by a former CIA agent in an article written for *Time* magazine, contractors constitute around 50 to 60 percent of the CIA's workforce.[15] Today around 80 percent of the approximately 45,000 contract workers employed in the field of intelligence in the United States belong to five private corporations: Booz Allen Hamilton, CSRA, SAIC, CACI International, and Leidos. All five companies are located in Virginia and are also involved in the development of hacking tools and cyber warfare.[16]

Lack of supervision, monitoring, and control

In contrast to intelligence, espionage, and cyber agencies that are subjected to partial supervision by parliamentary committees and congressional bodies, actions of privatization, outsourcing, and the transfer of sensitive activities to private hands are done without government supervision and control while regulatory bodies do not have the ability to examine the degree of legality when they are carried out by private entities. Furthermore, private companies may feel less of an obligation to provide full and reliable information to regulatory and supervisory bodies. In addition, many countries have laws that direct security and intelligence agencies how to carry out tenders, sign

[14] Simon Chesterman, "'We Can't Spy . . . If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Function,'" *European Journal of International Law* 19, no. 5 (November 2008): 1056, https://doi.org/10.1093/ejil/chn055.

[15] Robert Baer, "Just Who Does the CIA's Work?," *Time,* April 20, 2007, http://content.time.com/time/nation/article/0,8599,1613011,00.html.

[16] Tim Shorrock, "Why does WikiLeaks keep Publishing U.S. State Secrets? Private Contractors," *Washington Post,* March 16, 2017, https://wapo.st/2WkVO3M.

contracts with private companies, and complete the purchase of products or services; in most cases, however, these laws do not include a clear and precise definition of processes for supervising the hiring of outsourced companies or monitoring their conduct or that of their employees. Contract workers in the cyber field still must meet minimum security clearance conditions, a process that in the United States is known as long and slow and is affected by arguments over budgets between the Department of Defense and the Office of Personnel Management. This has resulted in a lack of competition among the contractors themselves, including among US intelligence and cyber agencies. Although cyber agencies in the US defense forces need the ability to quickly hire new employees, the slow process of providing security clearance has led to a rising demand for former employees with security clearance, thus causing a lack of competition between the contractors.[17]

A tender issued by the NSA to develop the Trailblazer system for mining data from cellular and email communication manifests the absence of competition in the private market regarding the development of cyber and intelligence gathering tools. The tender was awarded to SAIC in 2002, for 280 million dollars. By 2005, however, the cost of the project had ballooned to over a billion dollars, and the project was later described as a total failure. Nonetheless, when the NSA announced the ExecuteLocus program, whose aim was to replace the Trailblazer system, the contract was again awarded to SAIC despite its previous performance.[18]

Another issue in terms of outsourcing relates to defining which functions are reserved only for government and defense agencies and which can be privatized.[19] The contract for translation services signed with the contractor CACI International is an example of this problem. The company provided interrogators to the military police, which was responsible for the interrogation of Iraqi prisoners during the invasion of Iraq in 2003. According to an investigation that began in 2008 following a lawsuit filed against CACI, the company's interrogators reportedly abused prisoners and violated human rights.[20] This incident provides an example for awarding an out-of-scope

[17] Chesterman, " 'We Can't Spy…If We Can't Buy!,'" pp. 1068–1069.

[18] Ibid., p. 1058.

[19] Voelz, *Managing the Private Spies*, p. 23.

[20] James Lesher, "Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace," *Journal of Contract Management* (Summer 2014): 7.

function to contractors which are not accountable and are not supervised. Another problem is the lack of supervision of the nature and scope of activities that can be privatized, which can lead contractors who are carrying out research, development, information gathering, and sometimes even internet operations to change the incentive for their activity out of commercial interests. These commercial interests, such as maximizing profits or extending contracts, along with conditions that are contrary to those of the free market—such as a lack of information and lack of competition—can harm their activities and results. For example, commercial interests can lead to biased conclusions or intelligence analyses in order to appease politicians or people within the intelligence agencies themselves. In the year before the invasion of Iraq, the Center for Counterterrorism Technology and Analysis, which was managed by the contractor SAIC, produced intelligence reports detailing the existence of Iraq's weapons of mass destruction and its intention to start a war. With the invasion of Iraq, SAIC was awarded contracts for intelligence and defense activities on Iraqi soil.[21]

Another possible result of the lack of supervision is mismanagement of information security. The threat of the proliferation of cyber weapons could significantly increase as long as employees who have access to source codes of programs or of development projects are not supervised. The absence of government supervision and control could enable the employment of people who do not see their work as a national mission, which could lead to negligence or the employment of people who have ideologies which may undermine the implementation of their tasks. Such situations could lead to leaks of classified information, attack and hacking components, and more. Although much has been said about cyber threats by other national actors, such as Russia, China, North Korea, and Iran, to critical infrastructure, economic sectors, companies and governments in the West, inadequate information security or hiring candidates who are not suitable for security positions, along with a lack of supervision and accountability, could lead to a situation in which cyber weapons developed by the best minds are leaked or stolen. This problem is exacerbated by the difficulty in monitoring and supervising malwares and exploits.

[21] Donald Barlett and James Steele, "Washington's $8 Billion Shadow," *Vanity Fair* (March 2007), https://www.vanityfair.com/news/2007/03/spyagency200703.

These weapons could reach hostile parties and could be utilized against the very countries that had developed them in the first place, or against their allies. The leak of cyber weapons could enable countries with relatively low technical capabilities, terrorist or criminal organizations to carry out reverse engineering or to copy parts of code from sophisticated malware and reuse the stolen weapon.[22] For example, the Stuxnet worm, which was originally used to damage Iran's nuclear facilities, reportedly was copied and used for attacks on command and control systems in around fifteen power stations and chemical factories in Germany.[23]

Given these situations—in addition to the classification and compartmentalization practiced within cyber agencies—government bodies or organizations could be unaware of these problems, lacking the ability to impose policy or security standards on contractors, or could prefer the financial savings of hiring contractors. Examining the practice of outsourcing in the fields of intelligence and cyber reveals that, in addition to its advantages, it also has disadvantages (see Table 1 below), many of which surround the question of supervision and responsibility placed on contractors.

Table 1: Advantages and Disadvantages of Outsourcing in the Field of Intelligence and Cyber

Advantages	Disadvantages
Coping with budget cuts and personnel quotas	Competition between the private market and intelligence agencies
Surge capacity for coping with new and changing threats	Lack of competition between contractors
Access to advanced technology and rapid development	Lack of supervision over the types of processes and activities privatized
Increasing room for deniability (when using contractors for espionage operations or offensive cyber operations)	Potential for the politicization of processes and activities
Providing free rein—activity without legal constraints	Negligent or malicious management of information security and classified materials

[22] Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," 50, 59.

[23] Nicole Goebel, "Report says Stuxnet Computer Virus Hits German Firms," *Deutsche Welle*, October 2, 2010, https://bit.ly/2Z4fgPq.

Leaks of Cyber Weapons and Classified Materials: Case Studies from the American Intelligence Community

The Edward Snowden Affair

Background: The most infamous leak of classified material in recent years has been the Snowden affair. Edward Snowden was employed by the contractor Booz Allen Hamilton in 2013 and worked as an analyst for the NSA. In May 2013, about four months after he began his employment at Booz Allen, Snowden flew to Hong Kong, where, about a month later, he disclosed hundreds of thousands of classified NSA documents. These documents were published in the *Washington Post* and the *Guardian*, and afterwards by the *Der Spiegel* and the *New York Times*.

The connection between the incident and the proliferation of cyber weapons: Snowden's leaks disclosed the NSA's cellular communication and email correspondence surveillance techniques and capabilities. This included the disclosure of the PRISM program, which enabled the NSA to access Google and Yahoo data centers and extract information on civilians around the world, including American citizens.[24] Snowden's documents also disclosed databases of information gathered on civilians; information on analytical tools for gathering information from internet traffic; and information on the NSA's cooperation with communications companies and intelligence agencies of US allies.[25] Although most of the documents that Snowden leaked included information on the NSA's surveillance programs, it did not include the source codes of the components that were used for them. Nonetheless, the Snowden affair is a case that demonstrates the risk inherent when contractors are not supervised.

The motive: In several interviews given after leaking the documents, Snowden claimed that he did it out of a belief that the NSA's surveillance activity is illegal and violates the rights of American citizens. In addition,

[24] Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post*, October 30, 2013, https://wapo.st/2WMEmoA.

[25] Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *Guardian*, July 31, 2013, https://bit.ly/2s5QlvF; Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 6, 2013, https://bit.ly/2brf9H0; Scott Shane and Ravi Somaiya, "New Leak Indicates Britain and U.S. Tracked Diplomats," *New York Times*, June 16, 2013, https://nyti.ms/2YXifsS.

he accused the Obama administration of turning a blind eye to the espionage programs that began during the presidency of George W. Bush.[26] In this context, we can define Snowden's motives as ideological, which raises questions about the process of recruiting and placement of employees of contractors who are hired by US intelligence.

Harold Martin and the Shadow Brokers Leak

Background: Harold Martin was arrested in August 2016 on suspicion of taking home without any authorization around fifty terabytes of classified materials belonging to the NSA, CIA, and US Cyber Command. Martin had been employed for twenty years as a contract worker for seven different contractors who carried out projects for the Department of Defense, the CIA, and the NSA. In his last position, Martin had been a contract worker for Booz Allen Hamilton (for which Edward Snowden also worked). According to the indictment, Martin started stealing classified materials in 1996 and continued doing so until his arrest two decades later. Among the materials stolen were hacking components, documents describing techniques for hacking into foreign networks, and documents that detailed offensive cyber capabilities, processes and methods for gaining access to networks, and for protection of governmental systems and networks.[27]

The connection between the incident and the proliferation of cyber weapons: During the investigation, it was found that numerous materials that Martin had stolen were later found among the files leaked by the hacker group known as the Shadow Brokers.[28] These files were posted on the website Medium at the beginning of 2017 and included information on security breaches in systems and applications, along with details on methods of surveillance of computer systems, telephones, mobile devices, and websites.

[26] Barton Gellman and Jerry Markon, "Edward Snowden Says Motive behind Leaks was to Expose 'Surveillance State,'" *Washington Post*, June 10, 2013, https://wapo.st/2JSMJbU.

[27] Richard Chirgwin, "Ex-NSA Contractor Harold Martin Indicted: He Spent 'Up to 20 Years Stealing Top-Secret Files,'" *The Register*, February 8, 2017, https://bit.ly/2kuvq3f.

[28] Scott Shane, Nicole Perlroth, and David Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to its Core," *New York Times*, November 12, 2017, https://nyti.ms/2zznVzP.

The most prominent hacking component that allegedly had been stolen from Martin's computer was EternalBlue. EternalBlue is a code that exploits a vulnerability in the SMB (server message block) protocol, which is used for remote access of Windows operating systems. Since it was leaked, this component has been used for the spread of the WannaCry cyberattack, which affected over 230,000 computers in over 150 countries in May 2017.[29] EternalBlue continues to be commonly used around the world. According to a report by the Cyber Threat Alliance, an organization that shares intelligence on cyber threats, hackers continue to make use of this component in order to mine digital currency.[30] In this context, it should also be noted that the NotPetya global cyberattack was caused by using another NSA component called EternalRomance.[31]

Another example of a hacking tool that was leaked by the Shadow Brokers and may have been originally stolen by Martin is the DarkPulsar malware, which creates a backdoor and enables the installation of additional malware. In October 2018, Kaspersky Lab claimed that it had identified around fifty victims that were infected by DarkPulsar in nuclear energy, communications, IT, aerospace and research and development industries in Russia, Iran, and Egypt.[32]

The motive: At the time of this writing, the trial of Martin, whom his attorney has described as a compulsive hoarder, was still taking place and it had not yet been proven whether he sold the materials that he collected or whether they were stolen from his personal computer. Nonetheless, given that Martin took materials home over the course of years, it can be assumed that his conduct was negligent and improper vis-à-vis information security. In this context, many questions can be raised about the security measures of Booz Allen Hamilton, which did not discover Martin's actions even after

[29] "EternalBlue – Everything there is to Know," *CheckPoint*, September 30, 2017, https://research.checkpoint.com/eternalblue-everything-know/.

[30] "The Illicit Cryptocurrency Mining Threat," *Cyber Threat Alliance*, p. 14, https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf.

[31] Iain Thomson, "Everything you Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide," *The Register*, June 28, 2017, https://bit.ly/2tjXLhX.

[32] Catalin Cimpanu, "Kaspersky Says it Detected Infections with DarkPulsar, Alleged NSA Malware," *ZDNet*, October 19, 2018, https://zd.net/2OAL911.

it supposedly had increased its security measures and processes following Snowden's leaks.

The Vault 7 and Vault 8 Leaks from the CIA

Background: On March 7, 2017, WikiLeaks began posting a series of documents detailing CIA techniques, tools, and capabilities for carrying out electronic surveillance and cyber warfare. The series was called Vault 7, and the documents included were publicized in twenty-four parts between March and September 2017. In November of that year, the founders of WikiLeaks began leaking another collection of documents, which were called Vault 8.

In August 2017, Joshua Schulte was arrested as part of an FBI investigation into the distribution of pedophilic content. In a raid on his apartment, the investigators confiscated computers, mobile devices, and servers that contained pedophilic materials, as well as some classified material that he had taken from his workplace. Schulte worked as a software engineer for a CIA unit responsible for the development of codes for espionage programs and access operations. Schulte was not a contract worker, as initially had been estimated. During the investigation, it became clear that beginning in 2013, Schulte had uploaded a number of projects and codes that he wrote for the CIA to his public GitHub account, and had saved additional material on public servers for file-sharing.[33]

The connection between the incident and the proliferation of cyber weapons: the Vault 7 leaks throughout 2017, included hacking components for Linux and MacOS X operating systems for the purpose of espionage and information theft, as well as components used for intercepting communication, routing internet traffic, and shutting down security cameras.[34] The Vault 7 leaks mainly included documents describing hacking techniques and how to use hacking components. In contrast, the Vault 8 leak included source

[33] Jason Koebler, "Alleged CIA Leaker has some of the Worst Opsec I've ever Seen," *Motherboard*, May 17, 2018, https://bit.ly/2IxR2ZP; John Walcott and Mark Hosenball, "CIA Contractors Likely Source of Latest WikiLeaks Release: U.S. Officials," *Reuters*, March 8, 2017, https://reut.rs/2QDdodm.

[34] Pierluigi Paganini, "WikiLeaks – CIA Developed OutlawCountry Malware to Hack Linux Systems," *Security Affairs*, July 1, 2017, https://bit.ly/2uvnXTt; Sooraj Shah, "WikiLeaks Reveals CIA Tool Acting as SMS Proxy on Android," *Infosecurity-Magazine*, July 14, 2017, https://bit.ly/2vB7KfV; Swati Khandelwal, "3 New CIA-Developed Hacking Tools for MacOS & Linux Exposed," *Hacker News*, July 27, 2017, https://bit.ly/2BBfGRP.

codes and development records of the Hive project—a component that was used by the CIA to remotely control malware and receive information and data stolen from computers, whose existence had already been disclosed in the Vault 7 leak.[35]

The motive: The indictment against Schulte attributed his actions to malicious intent and an attempt to harm American national security. It claimed that Schulte gained unauthorized access to CIA computers from which the materials were stored, voluntarily transferred them to a third party, covered his tracks, blocked access by others to the system, and lied to his investigators.[36] Unlike Martin, Schulte denied these actions and claimed that he left the CIA as a result of an inability to continue to function, and as a result, the agency claimed that he was disgruntled and had turned him into a "scapegoat."[37] As of the time of this writing, it is not possible to know for certain what Schulte's motive was, but it is presumed that he had an active part in leaking the material which was publicized.

The Kaspersky Affair and the NSA Leak

Background: Nghia Hoang Pho worked as a developer for the TAO (Tailored Access Operations) division for developing hacking tools for the NSA from 2006 to 2015. Pho was accused of taking home classified digital materials and documents over the course of five years. His activity was discovered after Israeli hackers hacked into the computers of the Kaspersky Lab company and identified codes for NSA programs stored on them. The investigation showed that a Kaspersky anti-virus program that scans the computer and monitors malicious codes had been installed on Pho's computer. The anti-virus program had identified codes for NSA hacking programs that Pho took

[35] Swati Khandelwal, "Vault 8: WikiLeaks Releases Source Code for Hive – CIA's Malware Control System," *Hacker News*, November 9, 2017, https://bit.ly/2zKk3dj.

[36] "Joshua Adam Schulte Charged with the Unauthorized Disclosure of Classified Information and other Offenses Relating to the Theft of Classified Material from the Central Intelligence Agency," *Department of Justice*, June 18, 2018, https://bit.ly/2TuWMEU.

[37] Matt Zapotosky, "Ex-CIA Employee Charged in Major Leak of Agency Hacking Tools," *Washington Post*, June 18, 2018, https://wapo.st/2HTjKTf.

home as malicious and had sent them to a cloud folder that the company uses for research purposes.[38]

The connection between the incident and the proliferation of cyber weapons: As mentioned, Pho had worked for the TAO unit, which develops codes for hacking tools. The codes that the Kaspersky software collected from his computer belonged to projects that he had worked on and were identified as malicious codes. The investigation showed that, contrary to the claims of Kaspersky Lab, the information from Pho's computer reached Russian intelligence officials. There are three main theories about how the information was transferred from the Kaspersky software to Russian intelligence. One theory is that Russian hackers exploited security vulnerabilities in the Kaspersky software. The other theory holds that Russian hackers intercepted the information while it was being transferred to the Kaspersky server in Moscow, and the third theory is that Kaspersky Lab worked for the Russian government, and from the moment the materials were discovered on Pho's computer, it actively stole them and transferred them to Russian government officials.[39]

The motive: Pho confessed and claimed in a letter submitted to the court that he suffered from social problems and that he had taken the materials home in order to go over them outside of work hours and to improve his performance at work as well as in the annual performance grade given to NSA employees.[40] Pho's case reveals negligence and deficient information security and neither malicious intent nor an ideological motive.

Ways of Addressing the Disadvantages of Outsourcing

Given the increasing scope of the phenomenon of outsourcing and its many advantages, outsourcing will likely continue to expand. Therefore, the focus should be on solutions for minimizing its negative impacts.

In order to address the problem of leaks of vulnerabilities and cyber weapons by both regular employees and contract workers who work for intelligence and cyber agencies of the defense apparatus, governments and

[38] Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *New York Times*, October 10, 2017, https://nyti.ms/2g9jlRt.

[39] Zack Whittaker, "What is Kaspersky's Role in NSA Data Theft? Here are Three likely Outcomes," *ZDNet*, October 9, 2017, https://zd.net/313DdIr.

[40] Sean Gallagher, "NSA Employee who Brought Hacking Tools Home Sentenced to 66 Months in Prison," *Ars Technica*, September 26, 2018, https://bit.ly/2NHPOOk.

cyber security industries need to develop a defensive response. In addition, both the agencies responsible within the defense apparatus and the private contractor companies should be given more stringent supervision, with emphasis on the cyber security of systems and security procedures. Employees should undergo regular background checks, personal interviews, and their public records as well as their behavior on social media should all be checked. This information could shed light on employees' ideological or political views, which could affect their work performance. In addition, employees should also be required to undergo periodic medical and psychological tests, as these tests could help prevent any improper behavior.

Improving procedures and instituting recommended work practices for maintaining cyber hygiene can help to minimize negligence and unintentional leaks by employees. In order to improve the cyber hygiene of employees who develop or operate hacking tools and offensive cyber components, contract workers and employees of the defense and cyber agencies should be required to undergo periodic training and exams on identifying information security risks and cyber threats. In addition, procedures for working with classified information, including source codes and exploits, should be fine-tuned. Another possible solution for mitigating the theft of sensitive information, is a trend that has already begun in the United States and involves prohibiting defense and cyber agencies employees from using products of companies which hold connections to foreign governments, such as Kaspersky Lab's anti-virus products as well as communications equipment and devices of Chinese companies, such as Huawei and ZTE, which are obligated by Chinese law to cooperate with requests for assistance from China's intelligence agencies.[41] Security clearances should be made conditional upon abiding by these procedures and processes.

Minimizing negligence and information leaks can also be done with technological means. Technological solutions can help improve supervision of the cyber hygiene of employees or of contractors who work for them and include programs for scanning and monitoring external storage devices connected to the computers of cyber agencies or external companies, and scanning USB connections for any violations of information security and

[41] Arjun Kharpal, "Huawei Says it Would Never Hand Data to China's Government. Experts Say it Wouldn't Have a Choice," *CNBC*, March 4, 2019, https://cnb.cx/2EMfgMr.

for copying materials. Tracking the movement of files on networks and monitoring the email accounts of employees could improve supervision capabilities and help maintain cyber hygiene.

In order to combat improper conduct specifically by contract employees, economic incentives can be included in contracts signed with contractors, thus encouraging them to track, monitor, and supervise their employees and their activity, and to engage in more meticulous and in-depth personnel recruitment processes. These incentives could be included as a condition for participating in future tenders or for ending contracts if not fulfilled.

Even after implementing these suggestions, however, it will be impossible to completely prevent leaks. According to the director of the National Counterintelligence and Security Center, William Evanina, the focus should be on how to identify leaks as quickly as possible and thus minimize their damage from the moment they are discovered.[42] Therefore, the bodies responsible for cyber within the intelligence and defense communities need to carry out risk assessments that include scenarios in which the source codes of cyber weapons are leaked and work to understand the extent of the damage and impact of potential leaks on future operations, along with their potential impact on cyber stability. Once programs that could be used for extensive global attacks have been leaked, the community of cyber agencies must be prepared to disclose quickly and discreetly the security vulnerabilities to the manufacturers.

Conclusion

A review of the case studies shows that while contract employees have been linked to cases of poor information security, negligence, deficient cyber hygiene, and have even expressed opinions or had ideological background that are incompatible with the security-oriented nature of their work, internal employees of the cyber agencies have also been responsible for the illegal proliferation of cyber weapons. Thus, negligence, lack of regulation, and the employment of people with a problematic background or who are incompatible with the nature of the work can be found both among contractors and among the internal employees of the intelligence and cyber agencies.

[42] Patrick Tucker, “Can the NSA Stop the Next Snowden?” *The Atlantic*, September 18, 2016, https://bit.ly/2XliVru.

Outsourcing especially in the field of cyber has many advantages. Furthermore, the trend of outsourcing in this field is expected to expand and could even include carrying out offensive cyber operations. Nonetheless, the negative implications of outsourcing should not be overlooked, whether it is the leakage of offensive cyber capabilities and codes for hacking programs, or classified documents that disclose capabilities, methods, or operations. Even defensive actions carried out by private companies for government agencies, such as monitoring internet traffic and penetration testing, can be used for malicious purposes given a lack of supervision or negligence.

In order to address these problems, governments and cybersecurity industries must find a defensive solution that can handle the leaking of vulnerabilities, security breaches, and cyber weapons developed or used by contractors working for intelligence and defense agencies. This solution should include strict supervision of employees involved in developing and operating cyber weapons, including their undergoing periodic medical and psychological tests, comprehensive background checks, undergoing training and taking exams on the identification of cyber threats, and prohibiting the use of products manufactured by companies that have connections to foreign governments, especially strategic adversaries involved in cyber espionage. The use of technological aids can also minimize the negative impacts of the phenomenon.

Nonetheless, it seems that it will be impossible to completely prevent leaks of classified materials, including cyber weapons. Therefore, the cyber agency community must be prepared to identify leaks and cope with their potential damage the moment they are discovered.