Commercial and Industrial Cyber Espionage in Israel

Shahar Argaman and Gabi Siboni

Cyberspace is especially suited to the theft of business information and to espionage. The accessibility of information, along with the ability to remain anonymous and cover one's tracks, allows various entities to engage in the theft of valuable information, an act that can cause major damage. Israel, rich in advanced technology and a leader in innovation-based industries that rely on unique intellectual property, is a prime target for cyber theft and commercial cyber attacks. This article examines the scope of cyber theft and cyber industrial espionage globally, and attempts to estimate how much financial damage they cause in countries around the world and in Israel. It seeks to raise awareness of the extent of the phenomena among the relevant authorities in Israel and provide recommendations on how to grapple with it.

Keywords: Cyber, espionage, industrial espionage, intellectual property, cyber crime, cyber theft, technology

> *"There are two types of companies: companies that have been breached and companies that don't know they've been breached.... The vast majority of companies have been breached."*[1]
> Shawn Henry

> *The director of the National Security Agency, Gen. Keith Alexander, called cybercrime "the greatest transfer of wealth in history." The price tag for intellectual property theft from U.S. companies is at least $250 billion a year.*[2]

Shahar Argaman is the director of the National Cyber Staff. Col. (ret.) Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and Cyber Security Program at INSS.

Background

Cyberspace is a product of the accelerated pace of technological developments in the last few decades. Initially, communications and computerized systems were linked together to function as local networks. These networks were later linked together to form a global medium of existence and activity. At present, cyberspace continues to develop on numerous levels: in the wealth of interconnected computerized tools, in the number and variety of networks, in the volume of information traffic, in the level of connectivity, in the variety of applications, and in the degree to which economic and social activity depends on cyber functions.

While cyberspace brings with it much positive potential and broadens horizons on every level of human activity, it also entails new threats and in effect presents a new arena for hostile activity, from the sabotage of information in cyberspace to damage to the physical world through cyberspace functions.[3] As the overall use of cyberspace increases, so too does the hostile activity within the arena,[4] which already includes a vast range of threats: denial of service, destruction of websites, exposure of personal information for the purpose of wielding influence or instilling fear, various types of crime, industrial and security espionage, and damage to national strategic infrastructures, databases, command and control systems, and even weapon systems.

By its very nature, cyberspace is a medium particularly well suited to espionage in general and commercial and industrial espionage in particular. Industrial espionage among commercial rivals is hardly a new phenomenon, but cyberspace allows simpler access than in the past to a great deal of information while allowing a high level of invisibility. The damage that can result from commercial espionage today is of unprecedented scope precisely because cyberspace is optimally suited to such activity. Another reason cyberspace has become a key means of espionage is that state-sponsored intelligence organizations use it in the pursuit of state-sponsored goals – political, security, technological, and economic – as do criminal outfits pursuing purely economic gain. Much information has emerged about cyberspace espionage between states, especially cyber skirmishes between the United States and China, indicating that commercial espionage has become a primary tool of states in general and the powerful ones in particular, serving as a weapon in their economic wars and pursuit of global dominance.

As a state rich in advanced technology, Israel is very much at risk. The vast amounts of information created by financial, scientific, and other institutions within the state are stored, moved, and managed in cyberspace, and are therefore accessible to a variety of attackers. In addition, the part played by innovation-based industries and unique intellectual property in the Israeli economy is highly significant. Israel is a global leader in startup industries, which by their very nature generate additional motivation for commercial espionage against Israel. Given that advanced persistent threats (APTs) are rarely discovered by standard security measures of commercial companies, Israeli companies, especially those developing unique knowledge, presumably constitute targets for commercial espionage and the theft of intellectual property, as is the case in other technologically advanced countries.

The purpose of this article is to examine the use of cyberspace for commercial espionage and theft of intellectual property. The article seeks to underscore the complexity in assessing the extent of these phenomena and the economic damage they cause. Finally, the essay seeks to analyze the scope of commercial espionage in Israel in order to raise awareness of the phenomenon in the public discourse and thereby promote action to curtail it and as a result contain the damage it incurs.

Cyberspace as a Medium for Commercial Espionage

While commercial espionage has existed since the dawn of history, the transition of much of the business world to the cyber realm has propelled commercial espionage to this arena as well. Indeed, cyberspace is ideally suited to espionage, particularly commercial espionage. It allows relatively anonymous activity, including convenient and safe transmission of vast amounts of information regardless of distance and national borders. At the same time, it is very difficult for the victims of espionage – be they commercial or government bodies – to detect its occurrence. Even if the victims are aware of the attack and identify the spyware used to effect it, it is hard for them to attribute the malicious action to a particular culprit and credibly establish the responsibility and identity of the attacker.

Commercial espionage in cyberspace costs very little compared to other means of intelligence gathering, and entails a low level of risk of exposure. Cyberspace espionage greatly reduces the need for agents to infiltrate the target, and thus intelligence entities throughout the world can amplify

their capabilities, in terms of intelligence gathering within cyberspace[5] and the integration of traditional forms of espionage with new capabilities in this sphere. As such, espionage becomes simpler for the attacker and more dangerous for the attacked. For example, espionage involving a mole working for the organization under attack becomes simpler in the cyberspace era: transmitting stolen information is easier and identifying its source is harder. Furthermore, law enforcement has a lenient approach to cybercrime, thus reducing the risk taken by those engaged in commercial espionage. A burglar caught breaking and entering a physical place of business to steal information will probably have to pay a much higher price than someone stealing the same information using a keyboard.

Commercial espionage may be defined as the unauthorized possession of confidential commercial information not revealed to the public at large, for the purpose of attaining a technological advantage or economic gain. Such information may include data on strategy, planning, technological innovation, product development processes, manufacturing and marketing processes, advertising campaigns, financial status, legal issues, key personnel, salary information, tenders and bids data, and more. Targets might include not only competing organizations but also academic research institutes and other entities possessing valuable information. Unlike information gathering from open sources, obtaining the information often entails criminal offenses. This activity is only one branch of a larger group of economic crimes, such as embezzlement, fraud, theft, disruption of business activity, and more. Commercial espionage by a state is usually intended to strengthen the state's own economy, to create an economic advantage for that state or a sector of its economy in relation to competing sectors around the world.

The rise in the scope of commercial espionage in cyberspace reflects the technological, economic, and social changes that have occurred in recent years and the corresponding manner in which information is created, moved, stored, and managed in economic and scientific organizations, including sensitive bodies. Throughout the world, almost all commercial and scientific records, even the most sensitive, are digitally stored and accessible to computer networks. Given this pattern and given the advantages currently available to hi-tech attackers such as state-sponsored intelligence organizations or sophisticated criminal syndicates, these groups can use cyberspace to carry out theft of commercial and business

information. Such thefts are on a scale that far outstrips any past commercial espionage, both in terms of the importance and sensitivity of the stolen information to its owners and in terms of sheer quantity.

Experience has shown that only a few companies can identify hi-tech attacks carried out by state-sponsored espionage organizations or sophisticated crime syndicates. Even fewer are capable of effective defense.[6] There are many examples indicating that even the most sensitive companies in the defense industry in the United States were relatively easy targets for commercial (or security) espionage through the internet by state-sponsored organizations, apparently out of commercial motives.[7]

A report by ONCIX (the Office of the National Counterintelligence Executive) to the US Senate[8] addressed the threat of theft of commercial information and key rivals carrying out such activity in the United States. China and Russia were described as having the highest capabilities in the field and being "the most aggressive collectors of US economic information and technology."[9] A July 2012 report to the Congress by the same agency[10] cites Congressional testimony by Director of National Intelligence (DNI) General James R. Clapper regarding the US intelligence community's national threat assessment. Clapper testified that intelligence agencies of enemy nations are systematically developing methodologies and technologies to challenge the capabilities of the administration and private sector in the United States that protect national and commercial secrets.[11] Indeed, the 2013 US threat assessment put cyber threats at the top of the list of threats facing the United States,[12] ahead of terrorism and the proliferation of weapons of mass destruction.

The Complexity in Assessing the Damage of Commercial Espionage

Given the very nature of commercial espionage, assessment of the damage it causes is difficult for various reasons, including first and foremost the methodological problem of quantifying the scope of damage resulting from the loss of intellectual property and the fact that only a tiny fraction of all advanced espionage activity ever comes to light. In testimony before a US government committee, Richard Bejtlich, Chief Security Officer at Mandiant,[13] a company specializing in incident response and computer forensics solutions and services for government, defense, and enterprise organizations, said that of the total number of sophisticated

espionage attacks originating in China investigated by his company, only 6 percent of the attacks were discovered by the targets. This indicates that a tremendous gap exists between the prevalence of the phenomenon and an accurate appreciation of the cost to the economy resulting from commercial espionage.[14] Furthermore, sophisticated organizations engaged in commercial espionage in cyberspace use specific spyware that are incapable of being identified, blocked, or neutralized by the standard defensive tools of most commercial enterprises. Today, cyberspace favors the attacker by a wide margin.

Many espionage agencies use cyberspace as a key information-gathering arena. The capabilities developed by security agencies for this purpose far outstrip current defensive responses to these threats. Furthermore, focused, dedicated attackers also enjoy the advantage of being able to learn about and even obtain the defenders' security tools,[15] enabling them to run simulations in order to identify the conditions under which they will not be exposed by the very security tools the defenders are using.[16] In addition, state-sponsored espionage is carried out by intelligence groups designed for this purpose, whereas effective defense requires comprehensive, state-sponsored activity that involves security outfits and non-security organizations from both the government and the private sectors – an effort that is, by nature, slow and cumbersome.

The FBI has estimated that for every incident of penetration into computer networks identified by a US company, one hundred similar incidents have occurred that the computer networks failed to identify.[17] A report by Mandiant published in February 2013[18] stated that the goal of the Chinese attack formation was commercial espionage and that in that year it had attacked 141 Western companies, primarily in the United States. This is an example of commercial espionage activity carried out by a state-sponsored body that had been operating for years and eluding public awareness until the publication of the report.[19] On the basis of this example, one may infer that other companies coming under attack by sophisticated formations almost always fail to identify the attack. Even on the rare occasion when they realize they have been attacked, the attack is not made known to the public and the economic and security implications are not studied in the overall national context.

In the few cases in which companies and other organizations realize they are targeted and even manage to identify the spyware installed on

their computers, they are hard pressed to assess the scope and type of information that has already leaked through their networks. Failure to protect the company's or organization's assets often means that those in charge of security in these outfits tend to downplay the damage caused by the espionage. When unknown software – that is, malware – is discovered on the company's computers, the natural inclination is to remove it and make sure that the system continues to work. Only rarely will a company carry out a comprehensive forensic investigation aimed at uncovering the true nature of the attack and identifying the tools used to carry it out, as such an investigation is very costly – both in financial terms and in terms of the time needed to carry out a forensic investigation, during which the company's computer communications are severely compromised. Even when a full, professional forensic investigation is successfully conducted and the company's management receives a full, reliable picture of the theft of commercial data, often the organization will prefer not to make the theft publicly known or will at least seek to minimize the damage assessment, in the hopes of reducing the damage to the company's reputation that would result from a complete description of the theft. Damage to the company's reputation would, of course, endanger the company's relationship with its shareholders, investors, suppliers, customers, and all other stakeholders.

Finally, there is an inherent difficulty in assessing the financial worth of intellectual property. Clearly it is not necessarily reflected in the value of the investment that went into creating it, and this is probably the most precise statement one can make on the subject. The value of future income denied to a company as the result of information theft through cyberspace is entirely subjective and grounds for wild speculation.

For these and other reasons, it is extremely difficult to assess the cumulative damage caused to an organization as a result of commercial espionage in cyberspace. This difficulty is intensified when one tries to assess the financial damage the phenomenon causes the state, and thus assessments of damage to the state from commercial espionage in cyberspace vary wildly.

Methods of Assessing Commercial Damage

Various studies of the costs of commercial espionage have attempted to propose methodologies for damage assessment. The vast gaps in knowledge stemming from the above mentioned reasons as well as the

inherent difficulty in closing those gaps pose an obstacle to any attempt to assess the scope of the phenomenon.

It is customary to divide the cost of cyberspace crime into three main categories:[20] *defense cost*, such as security, compliance with standards, and insurance; *direct cost*, such as damage to functionality, repair of the damage, loss of work time, resolution of the breaches, reconstruction of information, direct losses to the business, compensation to customers, fines, and legal issues; and *indirect cost*, such as loss of customer trust, loss of future business and income, or damage to the company brand.

The various approaches to damage assessment are based on surveys and theoretical analyses. In the studies based on surveys, sample groups of executives and IT specialists in commercial ventures are asked to provide damage assessments, from which overall assessments are extrapolated. The problem with this approach is the profound gap between the respondents' understanding of the issue and the scope of the phenomenon in practice. This gap is even more pronounced given that the sample group is liable to be biased. Those who have suffered painful attacks tend not to share their experiences and are therefore likely not to participate in surveys of this type. Accordingly, the studies must correct for these factors, which in itself has a dramatic effect on understanding the scope of the phenomenon.

The theoretical approach uses a model based on calculations drawing on open data, hypotheses, and assessments by information security experts, businesspeople, economists, and law enforcement agencies. This model too suffers from a gap between the quality of available information and true data; it also relies heavily on assessments. One example of such research is a study of the cost of cybercrime conducted by Detica in England.[21]

Threat assessment and measurement are critical for understanding the phenomenon of theft in cyberspace and for the optimal allocation of resources to defend against it. Therefore it is in the best interests of both commercial enterprises and states to assess the damage they face from information theft. Gen. Keith Alexander, Commander of the US Cyber Command and the Director of the NSA, has claimed that US companies lose some $250 billion annually as a result of cyber theft of intellectual property.[22] Citing a report published by Symantec, he said, "Symantec placed the cost of IP theft to the United States companies [at] $250 billion a year, global cybercrime at $114 billion annually ($388 billion when you factor in downtime)."[23] A report by the Commission on the Theft of

American Intellectual Property estimates that the damage caused by cyber theft exceeds $300 billion a year.[24]

Countries other than the United States are also trying to assess the scope of the phenomenon. The Federal Office for the Protection of the Constitution in Germany assesses that German companies annually lose $28-71 billion and 30,000-70,000 jobs because of foreign economic espionage. South Korea has reported that the costs of economic espionage carried out by foreign entities in 2008 totaled $82 billion, compared to $26 billion in 2004. According to this report, 60 percent of the victims were small to medium-sized companies, and half of the cases of commercial espionage could be traced to China. In 2007, the Japanese Ministry of Economy, Trade, and Industry undertook a survey among 625 exporting companies and found that more than 35 percent of them reported the loss of some technology, and that more than 60 percent of the reported incidents were linked to China. Official sources in Great Britain have assessed that attacks on computer systems, including industrial espionage and theft of commercial information, cost the British private sector some $34 billion a year. More than 40 percent of this sum stems from the theft of intellectual property, such as specifications, formulas, and proprietary company information.[25]

Table 1: Assessments of Damage Resulting from Economic Espionage in Select Countries

Country	Assessment of annual damage (in $ billion) caused by theft of commercial information and intellectual property	Scope of damage in terms of percent of GNP
United States	250-300	1.67-2
South Korea	82	7.3
Germany	28-71	0.8-2
Great Britain	34	1.4

At the same time, those offering the estimates did not explain how they had arrived at their damage assessments, probably because of the difficulty in estimating the direct, not to mention the indirect costs of cybercrime. One must also take into account that those undertaking damage assessment studies, particularly certain information security companies, are liable to have a vested interest in inflating the scope of the phenomenon.

A study published by McAfee in July 2013[26] attempted to address the complexity of assessing the cost of cybercrime. The study questions published cost assessments and offers lower assessments than the official estimates of damage to the US economy. The study does not include definitive assessments of the cost of such damage, but points out, for example, that the upper limit of damage to the US economy claimed by one method of assessment is anywhere between 1/2 to 2 percent of the GNP,[27] whereas another method of assessment places it at lower than 1 percent of the GNP.[28]

Commercial Espionage in Israel

As a state rich in advanced technology, Israel is particularly vulnerable to threats in cyberspace in general and commercial espionage in particular. A great deal of Israeli export relies on companies highly dependent on intellectual property, thereby making Israel a target for the theft of this sort. Furthermore, the role of industries based on innovation and unique intellectual property in the Israeli economy is very significant. Israel is a global leader in startups, which invites further motivation for commercial espionage against Israel. In addition, the commercial sector in Israel has little awareness of the risks of cyberspace espionage and prefers convenience, functionality and exploitation of business opportunities rather than security. Presumably, therefore, as in other developed countries, commercial enterprises in Israel – especially those developing unique knowledge – are targets for commercial espionage and the theft of intellectual property. Of the 141 companies attacked by the Chinese attack formation APT1, as described by Mandiant, three were Israeli.[29]

Israel was a world leader when it came to understanding cyberspace-based threats to critical infrastructures, but not when it came to grasping cyber threats to the business world. As early as 2003, the state established the National Information Security Authority,[30] charged with securing Israel's critical infrastructures against cyberspace attacks and preventing the theft of state secrets. The Israeli business sector and the public at large did not benefit from similar attention, and currently no organization has the responsibility of protecting these entities against commercial espionage in cyberspace. As a result, Israel today lags behind many other countries in the world, including the United States, when it comes to protecting the business sector. Other countries reached the conclusion that state-

sponsored protection of national commercial assets is a high priority and that they are responsible for providing the scaffolding for responding to cyberspace threats to the economy in general and the private sector in particular. This realization has led to the establishment of one or several state agencies charged with leading state-sponsored defensive activity in cyberspace in order to strengthen overall protection in the field.[31]

It is hard to assess the damage caused to the Israeli economy by commercial espionage. There is no obligation to report the discovery of information-gathering tools in company computers, other than minimal guidelines for the population registry and regulation for special sectors, such as banks and bodies within the purview of the National Information Security Authority, and with respect to the authority overseeing security in the defense establishment. Furthermore, in Israel, companies are under no legal obligation to report the loss of sensitive business information,[32] and there is no organization charged with defending the business sector in cyberspace, whose job it would be to collect such information and use it in order to draw conclusions and strengthen overall defensive responsiveness. Consequently, the likelihood of identifying commercial espionage in cyberspace in Israel and accurately assessing its scope is very slim. This state of affairs presumably also accounts for the dearth of reports on theft of commercial information and intellectual property from Israeli companies.

Despite the difficulty of assessing the damage caused by attacks in cyberspace, Israeli businesses and organizations are presumably just as exposed to commercial theft as those of other developed nations, both because of Israel's image as a global leader in the development of innovative knowledge and because of the lacunae in defense and protections noted above. Even using conservative estimates – namely, that commercial theft in cyberspace accounts for one percent of the GNP – the annual damage of such crime in Israel reaches roughly $2.5 billion. Preliminary research on the damage of commercial espionage in Israel, undertaken for the National Cyber Command by Meidata, a market research company, assesses the annual damage to the Israeli market from commercial espionage to be in the $1-3 billion range. There is no doubt that damage on this scale, which increases from one year to the next, requires a national response and justifies significant investment in the defense of companies and

organizations under attack, which currently bear the lion's share of the cost of commercial espionage.

Conclusion

The State of Israel, with its high level of security awareness, was a pioneer in understanding the security risk developing in cyberspace, even before any damage to its critical infrastructures was actually identified. Nonetheless, to date the danger posed by the theft of trade secrets and intellectual property from commercial companies in Israel has not been recognized as a significant threat to the country's stability, even after clear evidence has emerged proving that nations and criminal syndicates, equipped with the most sophisticated tools in existence, use cyberspace to commit commercial espionage and that this state of affairs has far reaching economic ramifications for commercial companies and countries.

The economic threat to commercial companies from commercial espionage has been defined by the head of the US intelligence community as a concrete threat against the United States of the highest order, ranked ahead of terrorism and the proliferation of WMDs. The cost of damage incurred from commercial espionage in cyberspace is high and on the rise, and it is borne primarily by the business community. According to various studies, the component represented by the cost of commercial espionage is the most dominant in the total of all types of cyberspace crime.[33] Israel, whose economy is to a large extent driven by innovative knowledge, is also vulnerable to the threat of cybercrime, including commercial espionage.

It is very difficult to assess the damage incurred by commercial espionage in cyberspace. Therefore we see a very broad range of assessments generated by a variety of reports. The difficulty in assessing damage empirically and the extensive reliance on assessments by experts seeking to address major gaps in the quality of collected data constitute obstacles to all methods of assessing the damage caused by commercial espionage and account for the vast discrepancies among various damage assessments. Nonetheless, these assessments are necessary in order to understand the impact of commercial espionage, and they provide the basis for states' comprehension of the phenomenon and their attempts to thwart it.

A strong methodology that would provide the tools for reliable assessments of the damage discussed by this essay is highly necessary.

Development of this methodology would increase awareness of the need to improve protection against the threat and the ensuing damage. Toward this end, first and foremost it is necessary to improve the ability to gather reliable information about the phenomenon by means of mechanisms for reporting cyberspace incidents. Furthermore, it is necessary to develop better assessment tools that address existing gaps between reports and assessments surveying the number of incidents and resulting damage on the one hand, and reality on the other. This is an inherent gap in knowledge, because in most cases the attacked parties are not aware that they have been attacked and that information about their business has been stolen; they are therefore incapable, even after the fact, of linking damage to their business to information theft about which they knew nothing in the first place. In addition, improving the overall civilian responses in cyberspace in Israel, while also establishing an agency charged with responsibility for the matter, could allow for the development of a comprehensive doctrine for addressing commercial theft in cyberspace based on a broad view of national needs.

The goal of this essay is to shed light on the phenomenon of commercial espionage in cyberspace and the damage it causes to the Israeli economy. In the absence of in-depth studies of the phenomenon, its precise scope remains elusive, but it is reasonable to conclude that it has a significant impact on the Israeli economy and is steadily increasing. The response to the phenomenon must include a range of efforts, including but not limited to the following: focused research on the scope of the phenomenon and a breakdown by sector; improved security for the business sector; the development of a cyberspace security industry; and state-sponsored measures providing a response to commercial espionage throughout cyberspace, including cooperation and arrangement with other states suffering similarly from the phenomenon.

Commercial espionage in cyberspace demands a complex response and requires tremendous resources. Raising the level of awareness regarding the phenomenon, both in the business world and among the decision makers in Israel, appears to be a necessary precondition for engaging in efforts to reduce the damage caused by cybercrime in general and by commercial espionage in particular. It will then be possible to bring Israel's defensive cyberspace capabilities to bear against the entire gamut of threats.

Notes

1 Nicole Perlroth, "Nissan is Latest Company to Get Hacked," *New York Times*, April 24, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/?_r=0.

2 Carrie Lukas, "It's Time for the U.S. to Deal with Cyber-Espionage," *US News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.

3 For example, by making changes to computerized command and control systems of industrial processes so that damage is caused to the industrial process or to the industrial systems themselves.

4 Francois Paget, "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow," McAfee Labs, January 8, 2014, http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-cybercrime-and-hacktivism-will-continue-to-grow.

5 The most prominent example of surveillance carried out entirely in cyberspace is the global PRISM system of the NSA, whose existence came to light thanks to Edward Snowden's revelations. The NSA's surveillance was allegedly carried out for the sake of the security and safety of US citizens. However, there are reports charging that industries of interest to the United States, especially in the field of advanced security capabilities, were also placed under surveillance. See Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; and Scott Shane, "No Morsel Too Minuscule for All-Consuming N.S.A.," *New York Times*, November 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=1&_r=0.

6 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units," February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 See, for example, the successful cyber attack in 2011 on Lockheed Martin with the aim of stealing plans for the advanced F-35 stealth aircraft.

8 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, Annex B – West and East Accuse China and Russia of Economic Espionage*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

9 Ibid., p. 4.

10 *Foreign and Economic Espionage Penalty Enhancement Act of 2012*, House of Representatives Report 112-610, 2012, http://www.fas.org/irp/congress/2012_rpt/ecoesp.pdf.

11 James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence

Community for the Senate Select Committee on Intelligence," January 31, 2012, p. 8, http://www.intelligence.senate.gov/120131/clapper.pdf.

12 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence," March 12, 2013, http://www.intelligence.senate.gov/130312/clapper.pdf.

13 In January 2014 Mandiant was bought by FireEye.

14 Devlin Barrett, "U.S. Outgunned in Hacker War," *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

15 In most cases, the security tools are standard commercial tools.

16 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

17 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year," *International Business Times*, July 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559.

18 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

19 In the report, the company notes that it investigated dozens of advanced attack formations, of which more than 20 had similar characteristics and all originated in China. For reasons of its own, the company chose to relate to only one such formation in its report.

20 R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the Cost of Cybercrime," in *Workshop on the Economics of Information Security*, WEIS, 2012, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

21 Detica, *The Cost of Cyber Crime*, A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, UK, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.

22 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year."

23 Emil Protalinski, "NSA: Cybercrime is the Greatest Transfer of Wealth in History," *ZDnet*, July 10, 2012, http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/.

24 The IP Commission Report, *The Report of the Commission on the Theft of American Intellectual Property*, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

25 Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

26 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

27 Ibid., p. 14.

28 Ibid., p. 15.

29 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

30 The National Information Security Authority, established in accordance with a December 2002 government decision, is subordinate to Israel's General Security Services.

31 Overall responsibility for national defense in the United States falls on the Department of Homeland Security, which works in very close cooperation with the Department of Defense (which includes intelligence agencies, such as the National Security Agency and the Office of the National Counterintelligence Executive, that are very active in defending cyberspace against attacks and commercial espionage), the Federal Bureau of Investigation, and the Department of Justice.

32 Cyberspace theft from publicly held companies in Israel, which is liable to affect their activities or assets, might give rise to an obligation to inform the stock exchange, as such information could potentially affect the considerations of reasonable investors in deciding whether to buy or sell their company shares.

33 Detica, *The Cost of Cyber Crime*, p. 3.