Israel and Cyberspace: Unique Threat and Response

Matthew S. Cohen
Northeastern University

Charles D. Freilich
Harvard University
and
Gabi Siboni
Institute for National Security Studies

This article provides insights into the dangers and opportunities that the cyber realm poses to states by conducting the first comprehensive case study on Israeli use of cyberspace. Israel faces a constant barrage of cyberattacks from actors ranging from states to hacker groups to individuals. This has forced Israel to develop highly advanced capabilities. Israel has not just faced cyberattacks but has also been a leader in using the cyber realm for offense. Although the threats to Israel are severe, they are not unique; thus, Israel can serve as a model for what other states can do to effectively use cyberspace both defensively and offensively. This article offers policy recommendations as to how states can improve their cyber defenses.

Keywords: cybersecurity, cyber war, Israel, cyberspace

Israel, a state that relies heavily on cybertechnology, is particularly vulnerable to cyberattacks and has been a primary target thereof (Ben-David 2011, 57; Clarke and Knake 2012, 155). Indeed, Israel faces a nearly constant barrage of cyberattacks, roughly 1,000 every minute in 2012 (Eisenstadt and Pollock 2012; Grauman 2012, 66). During the 2014 operation against Hamas in Gaza, Israel faced over 1 million cyberattacks every day (Shamah 2014).

Although there is an ongoing academic debate (e.g., Demchak 2011; Nye 2011; Clarke and Knake 2012) regarding the actual severity of the cyber threat, and different countries have responded to it in various ways, Israel has taken it very seriously, defining the cyber threat as one of the gravest threats it faces and rapidly developing capabilities that have placed it at the forefront of the cyber world. Israel has been a leader in using the cyber realm for offense as well. Indeed, Israeli policies on cyber defense are trend setting and have been cited as an example of what the rest of the world should attempt to emulate (Grauman 2012). Major technology companies have taken notice of Israel's accomplishments and have established offices in Israel, and Israel additionally boasts a large number of start-up companies in the cyber realm (Eisenstadt and Pollock 2012, xiii, 32; Steinherz 2014).

Studies of national cyber policies have been conducted on only a handful of states, and there is no truly comprehensive academic study of Israeli policy and

Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2016) Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, doi: 10.1093/isp/ekv023

practice, a substantial lacuna. This article seeks to provide a comprehensive review of what Israel has done in the area of cybersecurity and cyberwarfare. On this basis, the article also seeks to provide recommendations as to what additional steps Israel could take to better protect itself and better utilize the cyber realm. Although the threats to Israel are severe, they are not unique, and therefore, in terms of offering policy recommendations, Israel's combination of innovation and danger makes it particularly worthy of study. All states have their own particular institutional and political constraints and opportunities, but Israel's example offers useful insights that can be molded to fit specific states and situations elsewhere. Finally, the article will contribute to the general understanding of the extent of the dangers and opportunities posed to countries by the cyber realm.

Existing academic research regarding Israel has largely focused on limited aspects of Israeli cyber policy (Farwell and Rohozinski 2012; Joint Advanced Warfighting School 2014). Even and Siman-Tov (2012) offer the most comprehensive examination of Israeli policy to date. They argue that cyberspace presents significant risks and benefits to Israel. On the one hand, Israel faces enemies that wish to cause it as much harm as possible and they are expanding their efforts into the cyber realm. On the other hand, Israel is a world leader in the cyber realm and has used this qualitative superiority, both economic and technological, to bolster its overall security and well-being.

In discussions of Stuxnet, the subject of much of the academic work on Israel and the cyber realm, most works have focused on the wider impact that such a virus may have on national security policies. Farwell and Rohozinski (2012), for example, offer analysis of how Stuxnet might impact national doctrines regarding the offensive use of cyber weapons around the world. An article by the US Army Command and General Staff College argues that Stuxnet demonstrates that cyber weapons may provide an effective means of creating physical damage (Parmenter 2013, 39). Even and Siman-Tov (2012) present an exploration of how viruses like Stuxnet could change the way foreign relations and warfare are conducted. They argue that, once deployed, such a virus can be modified and used by the targeted state. In contrast to these positions, Lindsay (2013) contends that Stuxnet can be understood as demonstrating the limits of cyber weapons. Attacks like Stuxnet marginally increase the power of stronger actors, but such viruses are so complex to build that they are difficult to launch. Finally, Sanger (2012) presents a detailed and comprehensive account of the Olympic Games program that led to the creation of Stuxnet and Flame, discussing United States–Israeli cooperation in creating them, and how and why they were deployed against Iran.

Clarke and Knake (2012) discuss the suspected Israeli cyber strike on a nuclear facility in Syria in 2007, as does Carr (2012). Both focus on describing how Israel conducted the strikes. Carr additionally discusses the motivations and actions of the groups and individuals targeting Israel and that Israel has launched counter-cyberattacks against Hamas and other Palestinian groups. Baram (2013) has written about how an increasing reliance on cyber tools by the Israel Defense Forces (IDF) might impact Israeli force buildup and military strategy generally. Carr (2012) argues that Israel, in fact, sometimes views the cyber realm as an alternative to conventional warfare as a means to achieving its goals. Parmenter (2013) builds on these understandings by discussing how Israel has used the cyber realm to enhance its ability to launch preemptive strikes both in the cyber realm and kinetically. Elran and Siboni (2015) describe how, in June 2015, the IDF began a two-year process that led to the establishment of a new Cyber Command. The command will integrate IDF cyber defense and offense with a focus on the importance of the synergy between these two disciplines. Elran and Siboni (2015) expect that this will be a challenging and complex process as current IDF cyber defense is the responsibility of the Telecom branch, whereas cyber offense is the responsibility of the Intelligence branch. Siboni and Assaf (2015) argue that the main goal of Israel's national cyber strategy should be to maintain the functional continuity of the state and recommend a set of measures to be taken toward this goal. They claim that the use of cyberattacks should not be limited to the strategic level but rather be enhanced to include capabilities on the operational and tactical battlefield (Siboni and Assaf 2015).

Many terms in the discussion of the cyber realm lack clear definitions; thus, for clarity, this article will offer definitions of some key terms. For the purposes of this article, a cyberattack uses and targets computers, networks, or other technologies for malevolent, destructive, or disruptive purposes (Libicki 2009, 23; Clarke and Knake 2012, 6; Valeriano and Maness 2015, 3, 32). Cyberattacks have two main motivations: political and criminal. Our focus is on cyberattacks against states and not on cybercrime, but much of what is argued applies to cybercrime as well. Politically motivated cyberattacks aim to provide a strategic, diplomatic, economic, or military advantage over an adversary and include efforts to disable critical military, governmental, or civilian networks, espionage, and efforts to infect systems with malware for future use. Cyberattacks often aim to force the target to take an action it does not want to (Hathaway et al. 2012; Valeriano and Maness 2015, 3). Cyberattacks on Israel also raise interesting issues with regard to attackers' political motivations. Many of these attacks are conducted without any specific demands in mind but are instead offshoots of wider campaigns aimed at undermining Israel's international standing, weakening it physically, or undermining its societal morale. While a limited number of cyberattacks are unlikely to force Israel to change its policies, the constant barrage is designed to force it to do so by disrupting daily life and governmental functions. In effect, it is warfare by other means (Carr 2012, 21–22).

Cyberattacks can be launched by states, nonstate actors, or individuals and can target military, governmental, or civilian systems. Cyberattacks may or may not involve physical damage. In cases where they do, the attack must cause the damage via an attack on one of the aforementioned systems, unlike in a kinetic attack where the damage done is direct (Singer and Friedman 2014, 69). A cyberattack, like a physical attack, can run the gamut from small-scale attacks, such as Distributed Denial of Service (DDoS) attacks, to major ones, such as attacks on the Iranian nuclear program that will be discussed subsequently.

Cyber offense overlaps with the concept of cyberattack. In essence, cyber offense refers to the tools (computer code) and strategies that a state, group, or individual employs to design and launch cyberattacks (Rid and McBurney 2012, 6; Valeriano and Maness 2015, 26, 33). Cyber defense involves the tools and strategies that states, groups, and individuals use to protect against cyberattacks. This includes such factors as whether a state controls its Internet service providers, how well it can control incoming and outgoing traffic, and how well it can halt ongoing attacks (Demchak 2011; Valeriano and Maness 2015, 26–7). Cyber espionage refers to the use of the cyber realm (often via malware or hacking, such as spear phishing) to steal, harass, gather information, or make known the attacker's ability to penetrate networks (Singer and Friedman 2014, 91–2; Valeriano and Maness 2015, 35, 68). Cyber espionage can be conducted by states, nonstate actors, and individuals. Targets include military systems (to gather intelligence on strategies, operations, and weapons design or to disable systems), government secrets, civilian infrastructure, and economic information (Singer and Friedman 2014, 93; Valeriano and Maness 2015, 26).

This article will provide an overview of the major attacks on Israel, followed by an examination of how Israel has defended against such attacks and engaged in the offensive use of cyber technology. These sections will include insights into how Israel detects, deters, and defeats adversaries and how Israel has begun to build greater cyber resilience. We also examine Israeli policies regarding research and development and human resources. These sections aim to provide insights into the ways in which Israel has developed strategies and institutions over time to effectively defend and promote its interests in cyberspace. Finally, the article will examine what can be learned from Israel's experience and the ways in which Israel can further improve its defensive and offensive use of cyberspace.

Cyberattacks in Israel

Foreign states, sophisticated hacker groups, and cyberactivists have attacked Israeli hospitals, the Tel Aviv Stock Exchange, the Bank of Israel, and government Web sites (Silber 2012). During the 2009 operation against Hamas in Gaza, Israel was hit with four waves of progressively stronger cyberattacks from over half a million computers (Herzallah 2009, 11). Israel suspected the attacks were paid for by Hamas or Hezbollah and conducted by an unknown organization in the former Soviet Union (Pfeffer 2009). Among the Web sites taken offline were the Israel Security Agency (ISA, or Shin Bet) and the Home Front Command, which instructs citizens how to protect themselves from rockets and other threats (Herzallah 2009, 11).

In 2011–12, a group linked to China's People's Liberation Army hacked three Israeli defense firms, apparently to steal blueprints of Israel's antirocket and antimissile systems (Vincent 2014). When again battling Hamas in 2012, Israel faced a sophisticated cyber operation aimed primarily at government Web sites (the offices of the president and prime minister, and the foreign and defense ministries). A total of over 100 million cyberattacks were launched during the campaign. As in 2009, the Web site for the Bank of Jerusalem was taken down, as was El Al's Web site, while the IDF's public site encountered problems and the Kadima party's was defaced (Hirshoga and Toker 2012; Khazan 2012; Zippori 2012). On the eve of Holocaust Remembrance Day in April 2013, hacker groups coordinated a series of cyberattacks entitled #OpIsrael to make financial, business, educational, nonprofit, and news sites inaccessible. During the 2014 campaign against Hamas, the Home Front Command Web site was again temporarily taken offline, as were some public IDF Web sites (Winer 2014). The Syrian Electronic Army was able to hack the IDF's blog and Twitter account and post its own images (Institute for National Security Studies and Cyber Security Forum Initiative 2014; Ruble 2014). In 2015, Anonymous threatened Israel with a so-called electronic Holocaust in which it would "erase" Israel from cyberspace, though in the end, the actual impact was limited to the defacing of just a few dozen Web sites, none of which were government Web sites (Moore 2015).

In 2011, Iran reportedly launched "Newscaster" against Israel, the United States, and other Western countries to gather intelligence by creating a series of false virtual identities with ties to government officials and reporters. The attack, which compromised over 2,000 computers, was only uncovered in 2014 (Perlroth 2014). Iran additionally appears to have been able to penetrate defenses in several government agencies and to have successfully accessed restricted information (Mandiant 2014, 8–9). In 2013, Israel accused Iran, Hamas, and Hezbollah of a series of large-scale attacks against "vital national systems," including water, power, and banking sites (Reuters 2013). During the 2014 Gaza campaign, Iranian attacks exceeded all previous ones, both in scope and breadth of the targets selected. The Iranian attacks mainly targeted civilian infrastructure, including financial networks, but also targeted government security systems, including, reportedly, an attempt to seize control of Israeli drones (Lappin 2014b; Soffer 2014).

Israel has faced attacks from Turkey, North Africa, and the Palestinians (Even and Siman-Tov 2012, 36). The danger from nonstate actors and cyberactivism by individuals and groups is also growing (Ben-David 2011, 57). Such operations are already capable of interfering with the government's ability to communicate instructions to the public in times of emergency, such as when the Home Front Command's public Web site was taken down by hackers during the operations in Gaza in 2009 and 2014. Cyberattacks pose additional dangers during security emergencies, and in fact, the frequency of attacks against Israel has been shown to increase during such situations (Even and Siman-Tov 2012, 37).

The Israeli Response to Cyberattacks

The cyber realm has long occupied a significant place in Israeli security thinking. Prime Minister Benjamin Netanyahu has stated that cyberattacks are "one of the four main threats to Israel" (Ravid 2014a). Former premier and defense minister Ehud Barak warned that "cyber warfare has taken asymmetric warfare to a new height, allowing a lone hacker to cause major damage" (Katz 2012a). Former general Yitzhak Ben-Israel, who served as chief advisor to Netanyahu on cyber issues, said that cyber-readiness is central to Israeli thinking, both offensively and defensively (Shackle 2012). The IDF views cyberspace as "a platform to improve operational effectiveness and defense" and as another potential battleground, much like the ground, sea, or air (Ynetnews 2012).

In 1997, Israel established Tehila (Government Infrastructure for the Internet Age), one of the first governmental cybersecurity agencies in the world, which aimed to ensure secure connections for government offices and secure hosting for government Web sites (Ravid 2011). In 2002, the Israeli government decided to establish the National Information Security Authority (NISA) for the protection of its national critical infrastructure. In 2011, the National Cyber Bureau was established, and the IDF recently created a new centralized Cyber Command (Opall-Rome 2015). There is, however, growing concern in Israel that despite its current advantages in the cyber world, other states and players will be able to catch up, and even if they cannot fully close the technological, strategic, doctrinal, and organizational gaps, they will come close enough in terms of capabilities to better penetrate Israeli defenses (Ben-David 2011, 57).

Israeli Defensive Cyber Organizations and Operations

Israeli cybersecurity activities aim to defend security organizations, government, critical national infrastructure, the private sector, and private citizens. The IDF is concerned that enemies will be able to penetrate, disrupt, take control of, and even use military communications networks against Israel, especially during hostilities (Katz 2012b, 2012c). Moreover, every major IDF weapon—including submarines, missiles, aircraft, and radar—has electronic components that are vulnerable to attack (Lappin 2013b). To this end, the IDF stresses "thwarting and disrupting enemy projects which may aim to target the Israeli military and government," and the IDF has been working to develop the ability to defend its communications and weapon systems (Ynetnews 2012).

In 2011, the National Cybernetic Task Force was established to review Israeli cyber policies and to recommend improvements designed to guarantee Israel's cybersecurity and global leadership in the field. The task force argued that it is essential to Israel's future that it continue to develop state-of-the-art cyber defenses to protect the economy and maintain a society that is democratic, open, and knowledge-based. To this end, the task force identified a number of overarching goals for Israeli policymakers: provide better information to the public regarding threats from cyberspace, develop better cyber training programs in schools and increase funding for them, improve governmental regulations, and expand investments in cyber research and development. The panel further advocated forming a national body responsible for determining cyberspace policies, expanding research grants, building a strong industrial base to safeguard Israel's cyber advantages, and increasing international cooperation in this area (Levi 2011). Another area of concern identified was the brain drain from the government to the private sector (UPI 2012). The main recommendation of the task force was the creation of the National Cyber Bureau (NCB).

The mission of the NCB is to promote and regulate government cyber activity, improve cyber defense for the non-defense-related sectors of the government (Ben-David 2011, 57; Efrati and Yafe 2012), and, especially, expand "the state's capabilities to secure critical infrastructure systems against cyber-terrorism, carried out both by foreign nations and by terrorist groups" (Even and Siman-Tov 2012, 79). The NCB was additionally charged with a wide range of tasks: recommending policy changes to the government with regard to cyberspace, including a national cyberspace security doctrine; promoting Israel's cyberspace industry; funding cyber research and development; promoting national cyber-educational programs; improving coordination and cooperation between government agencies as well as between the government and academia, industry, and the private sector; and holding national and international exercises to improve Israel's cyber-preparedness (Even and Siman-Tov 2012, 80–1; Israel Ministry of Foreign Affairs 2013; National Cyber Bureau 2014). The head of the NCB has stated that the NCB would also serve as a coordinating body for public and private groups in order to enable the pooling of resources and information in a single body capable of devising the best solutions possible (Baram 2013, 30–2; Israel Ministry of Foreign Affairs 2013).

Israel is in the process of establishing a Computer Emergency Response Team (CERT).[1] CERT will focus on the aviation, transportation, health, finance, and energy sectors and respond to computer security attacks, such as viruses, spam, and malware. CERT will also develop cybersecurity guidelines and provide recommendations to citizens, companies, and government agencies on means for improving their cybersecurity. Israel has additionally been engaged with private companies, particularly cell phone providers, to help them improve their defenses (Lappin 2013a).

Criteria have been adopted to determine which infrastructure facilities should be considered "critical" and, thus, be protected. Under these criteria, roughly 80 bodies are counted as "critical infrastructure," including some hospitals, heavy industrial plants, and energy, communications, and transportation companies (Ben-David 2011, 57; Lappin 2013a). Further, the Bank of Israel has assumed responsibility for ensuring the cyber defense of the banking sector and has required that banks develop plans for preventing cyberattacks and dealing with the aftermath of such attacks (Arutz Sheva 2012; Aizescu 2014; Supervisor of Banks 2015). The ISA contains a unit responsible for defending against cyberattacks on critical cyber infrastructure as they occur, including attacks from Iran and groups like Anonymous, and for running simulations of attacks so that Israel is prepared (Bergman 2012; Dvorin 2014). There has been tension, however, between the NCB and the ISA regarding which organization would be formally responsible for defending national cyberspace (Ravid 2014b). After lengthy debate and bureaucratic infighting, it was decided in September 2014 to create a new agency responsible for this under the overall guidance of the NCB (Ravid 2014a). The General Staff's C4I branch currently bears primary responsibility for defending all IDF communications and computer-based systems (Katz 2012b). The Ministry of Defense also has a cyber defense body to help protect the Israeli defense industry, and Mossad has reportedly built defensive cyber capabilities to address a wide range of threats (Katz 2012c; Bob 2013).

For years, the Telecom branch of the Ministry of the Treasury was responsible for ensuring the cybersecurity of Israel's various civil ministries and government computers. In 2015, Israel moved these responsibilities to the government's Telecom Authority, which is within the prime minister's office. The responsibilities have remained the same (Prime Minister's Office 2014).

[1] The tender to build CERT was awarded to a group of companies that includes IBM, EMC, Cisco, Matrix, and Rafael (Rafael will serve as the main contractor for the establishment of CERT's headquarters).

Detecting Attacks

Receiving early warning of impending attacks is critical in both the physical and cyber realms as it is far easier to defeat an attack before it occurs than after it has breached a network. Yuval Diskin, the former head of the ISA, has stated that Israeli cyber defense policy

> should be aimed at protecting not only networks, but also the single computer, as well as the whole of the communications entering the country.... We should not only protect against attacks, but also develop the means of identifying potential attackers and preventing them from operating (Ben-David 2011).

To this end, Israel has created units, reportedly including within ISA, that employ hackers who attempt to breach defenses in both the public and private realms (for example, banks, hospitals, and water) in order to expose potential vulnerabilities and fix them before they are attacked (Bergman 2012; Dvorin 2014). Such units can also provide valuable insight into how to identify enemy hackers (Bergman 2012; Lappin 2014a). CERT teams will also provide information on potential attacks, which could provide critical early warning. The IDF is additionally working to develop the ability to defend its communications networks and weapon systems and gather intelligence on parties that might have the ability to attack Israel's networks and systems (Lappin 2013a).

Active defense tools can be effective for preventing cyberattacks (Even and Siman-Tov 2012, 19; Sklerov 2012, 195); thus, Israel has developed systems that identify which Internet service providers (ISPs) and countries are most likely to be used to host attacks (to date Russia, China, Turkey, Saudi Arabia, and Iran). Israeli cyber defenders are given wide latitude in blocking certain ISPs from these countries when they detect an attack, even before it is clear which ISP is the source (Lappin 2013a).

In 2014, an Israeli defense contractor, Israel Aerospace Industries, opened a new research and development center in Singapore with the goal of developing new technologies and new techniques that will provide early warning of cyberattacks. The center will examine how to improve technologies that can identify attacks as they begin in real time, monitor them, and then redirect the attacks to Web sites set up to absorb them. It will also look to improve the detection of anomalies that might indicate impending attacks (Lappin 2014a).

Deterrence

Another means of preventing attacks before they occur is through deterrence. Israel appears to base its deterrence on both its defensive and offensive capabilities. Israel emphasizes its defensive capabilities in the hope that it will succeed in showing potential attackers, both state and nonstate, that their chances of success are limited and that it is not worth their time (Bob 2013). At the same time, as will be detailed in the next section, Israel has developed an impressive record of using the cyber realm for offensive purposes. These offensive capabilities aim in part to accomplish specific goals and likely to show potential attackers what Israel is able to do if it chooses to respond to an attack. It is not clear, however, whether Israeli deterrence has really been successful; the sheer number of attacks that continue today would suggest otherwise.

Israeli Offensive Cyber Organizations and Operations

In 2012, the IDF stated that, if necessary, it would be ready and able to use cyber weapons (Ynetnews 2012), although the nature of these weapons and the conditions under which Israel would use them remain unknown. As in other spheres, Israel neither confirms nor denies cyberattacks, at least partly because they are difficult to trace, thereby allowing it to avoid taking responsibility for them and lessening the chances of reprisal (Libicki 2009, 19; Egozi 2011, 6; Even and Siman-Tov 2011, 19; Nitzan 2011; Carr 2012, 252; Fulghum 2012, 29; Katz 2012c; Parmenter 2013, 3).

The IDF currently has two primary bodies dealing with the cyber realm, Intelligence Unit 8200 and the General Staff's C4I branch (command, control, computers, communications, and intelligence). Unit 8200, in many ways equivalent to the US National Security Agency, was entrusted with the IDF's offensive cyber capabilities in 2009 and reportedly created a new special "cyber staff" in 2011 to develop and deploy offensive cyber weapons (Ben-David 2011, 57; Katz 2012c). Funding and personnel for cyber programs within the military have also been increasing, including a new Office of Capabilities and Operations within Unit 8200 (Katz 2012b).

In June 2015, the IDF announced plans to create a unified Cyber Command by 2017. The new Cyber Command would integrate the functions of the C4I branch, Unit 8200, and military intelligence. All IDF offensive and defensive operations would be included under the Cyber Command. The creation of the Cyber Command will enable Israel to ensure that its defensive and offensive capabilities are fully integrated. The new unit will receive funding for existing units as well as additional priority funding as part of the IDF's new five-year funding plan (Opall-Rome 2015).

The Israeli cyber action that has received the most attention was the Stuxnet worm, which was reportedly launched in collaboration with the United States to attack Iran's nuclear program. The worm targeted the supervisory control and data acquisition systems of Iran's uranium enrichment centrifuges. Once a computer was infected, Stuxnet could alter information to hide its presence and cause damage until it was discovered (Fulghum 2010; Farwell and Rohozinski 2011, 25; Parmenter 2013, 45–9; Joint Advanced Warfighting School 2014, 14; Zetter 2014). Stuxnet apparently did achieve its intended goal, which was to delay the Iranian nuclear program, but it did not completely derail the program, which would have obviated the need for other measures such as possible military action (Farwell and Rohozinski 2011, 11; Sanger 2012).

Stuxnet was a useful tool because, unlike a physical strike that can only destroy known facilities, the worm was transferred to secret facilities about whose existence Israel and the United States suspected but did not have firm information on (Farwell and Rohozinski 2011, 25). Additionally, a physical strike on Iran would have been problematic for Israel to carry out owing to geography and Iran's likely response, so Stuxnet provided a unique opportunity to accomplish an important military goal with minimal risk. Stuxnet was likely the first cyberattack to inflict physical damage representing a new tool in warfare (Sanger 2012; Parmenter 2013, 39–40, 42–3; Joint Advanced Warfighting School 2014, 14–5).

Unit 8200 was reportedly involved in the development and use of malware for offensive purposes, such as the Stuxnet worm, and is reportedly working to develop the ability to sabotage critical infrastructures of potential enemies, particularly Iran (Katz 2012c; Silverstein 2012). Unit 8200 and the United States were reportedly also behind the Flame malware used against Iran, which took screenshots, recorded audio conversations, viewed network traffic, intercepted keyboard strokes, and likely stole information from infected computers while allowing all of this to be viewed remotely (Zetter 2012). Mossad is also reported to have developed offensive capabilities and to have worked with Unit 8200 to help create Stuxnet and Flame (Katz 2012c). Additionally, Lebanon has claimed that Israel hacked into its cellular telephone infrastructure to spy on it (Egozi 2011, 6).

Israel also has reportedly used cyber tools to support combat operations, such as the air strike on a Syrian nuclear reactor in 2007 (Clarke 2008, 310; Carr 2012, 51; Parmenter 2013, 35–8). In this incident, the Israeli Air Force apparently was able to fly into Syrian air space and bomb the reactor without alerting Syrian air defenses (Fulghum 2010). To accomplish this, Israel reportedly took control of Syrian radar systems and tricked them into thinking that nothing was happening, even while the attack was under way, and without alerting guards to the system's capture (Egozi 2011, 6). Israel chose not to blind the Syrian defenses, or shut them down, which would have alerted Syria to trouble, but instead temporarily reprogrammed the systems to make it appear that they were functioning normally (Egozi 2011, 6; Clarke and Knake 2012, 4–6).

The ISA has also developed both offensive and defensive capabilities in order to defend Israel from attack. The SIGINT and Cyber branches are the units responsible for cyber actions within the ISA, and the ISA a different set of responsibilities than those of the IDF. In both the physical and cyber realms, the IDF focuses on external enemies and military threats, while the ISA focuses on internal security. The ISA has devoted a great deal of effort to improving the ability to extract intelligence from computer networks, social media, and telephone conversations. Additionally, the ISA helps to protect national critical infrastructure and improve information security (Rapaport 2014).

Resilience, Research and Development, and Human Resources

To help ensure that Israel is ready to withstand and recover from attacks, it conducts drills to simulate cyberattacks such as the one conducted in 2012 by the NCB and the Counter-Terrorism Bureau. This drill, called Lights Out, tested the readiness of Israel's critical infrastructure defenses, as well as contingency plans during a cyberattack (Zitun 2012). In 2015, Israel decided to use its yearly home front defense drill, Turning Point, as a platform for a cyber-defense drill. During Turning Point 15, Israel simulated cyberattacks that brought down the electrical and telephone grids in order to improve its response during and after an attack (Times of Israel 2015). Despite these efforts, Israel has yet to conduct a full-scale operational drill that would simulate a massive and devastating cyberattack. Though NISA is charged with ensuring the resilience of Israel's national critical infrastructure, Israel has yet to develop robust resilience capabilities and methodologies on the national level that also integrate the civilian business sector. Importantly, a substantial part of physical resilience capabilities and strategy (for example, responses to kinetic attacks or natural disasters) are applicable to cyber resilience as well.

There are roughly 200–250 start-up companies in Israel dealing with the cyber realm and 20 research and development centers run by multilateral corporations, a number equal to the sum total of companies in this field worldwide, excluding those in the United States (Steinherz 2014; Ziv 2014). Israel additionally has between 7,000 and 8,000 engineers working in the cyber realm (Ziv 2014). As cyber defense impacts both the civilian and military sectors, there is relatively close cooperation in Israel between the cyber defense industry and the government (Even and Siman-Tov 2012, 22; Institute for National Security Studies and Cyber Security Forum Initiative 2014), as exemplified by the Advanced Technology Park (ATP) on the campus of Ben-Gurion University in Beer Sheba. Opened in September 2013, the ATP created a space in which government officials, academics, corporations, and the IDF could collaborate on cyber projects, share data, and assist each other with personnel, resources, and ideas (Levi 2011; Hiner 2013). The IDF C4I branch has been working with defense industries to create cyber simulators that will help train military personnel to protect critical military assets and networks (Israel Ministry of Foreign Affairs; Katz 2012b). Former members of Unit 8200 have also gone on to found numerous start-up companies.

The Israeli government and Israeli companies have also reached out to their counterparts in the United States to improve cybersecurity. Israel and the United States have worked together to create bi-national foundations aimed at supporting research and development in both countries. US and Israeli firms frequently partner, and many of the largest US technology companies have offices in Israel, including Microsoft, Apple, Cisco, IBM, and Google (Eisenstadt and Pollock 2012, xiii, 32). The NCB, as noted, has also been instructed to foster international cooperation (Israel Ministry of Foreign Affairs 2013; Baram 2013, 30–32).

Finally, in 2012, Israel began a new program designed to identify and train students aged 16 to 18 with exceptional computer skills (Jerusalem Post 2013). Recruiters reportedly scan the Internet for suitable candidates. The IDF can then offer such students the chance to attend one of its technical high schools, which funnel students to the IDF's cyber units (Silverstein 2012). In 2012, the IDF committed to spending hundreds of millions of shekels (3.5 shekels ≈ 1 US dollar) on cyber defense over a five-year period (Harel 2012). In April 2012, the IDF graduated its first "cyber defenders" from a year-long program in which the students were trained to examine IDF computers and networks in an effort to prevent and detect attacks (Katz 2012c), and in 2013, the IDF announced that the number of soldiers sent to cyberwarfare courses would be increased significantly. After passing these courses, graduates are then placed in the air force, navy, intelligence, and communications branches of the IDF (Cohen 2013).

The government is also attempting to improve enrollment in high school computer science classes (Levi 2011). Israel has roughly 1,000 trained computer science teachers in primary schools, making it a world leader (Economist 2014). Colleges and universities have also created or expanded cybersecurity programs, and private companies have begun to offer training to their employees. However, Israel has not yet figured out how to stem the brain drain from the government to private industry. There are not enough resources for higher salaries, meaning Israel will have to develop other incentives to convince people to stay (UPI 2012).

Conclusions and Recommendations

Israel already faces numerous cyber threats that continue to grow daily, as do those facing the world at large. Israel has responded to these threats by developing myriad ways to use cyberspace as a platform for promoting its interests, both offensively and defensively, and its policies and technology have made it a world leader in the field. Although Israel is at the forefront of crafting successful cyber policies, there is more that Israel can do to take full advantage of the cyber realm. Although Israel has been largely successful in mitigating the negative impacts of cyberattacks to date, the potential for damage in the future is great. An important starting point is identifying which attackers require the greatest attention.

As Israel's experience has demonstrated, it is possible to successfully defend against attacks by individuals and groups. States need to focus their efforts on preventing attacks by the few highly sophisticated actors, which are mainly states and a comparatively small number of terrorist and other organizations. In dealing with less sophisticated threats, states should aim to isolate hackers from resources and the broader community of hackers, for example, working with ISPs to disrupt or block a hacker's access to the Internet (Applegate 2012). Such a technique is most likely to be effective against individuals who rely on such connections to learn new methods and tools. This strategy is also effective against many nonstate actors whose members rely on similar communities to improve their skills.

Within the limitations of operational security, Israel should seek to deepen and expand the number of states it cooperates with on cybersecurity issues to improve

Israel's defensive and deterrent capabilities. Having agreements to share intelligence information on possible cyberattacks with other states also makes it easier to prevent and respond to them. Working with intelligence and law enforcement agencies in other states to prevent attacks or make attackers pay a legal price will strengthen deterrence against many forms of attack. Such cooperation is particularly important for Israel to develop as it is under constant attack and thus could benefit from any additional assistance it can garner. Along these lines, prominent former security figures in Israel have hinted that the cooperation between the United States and Israel in the cyber realm is not optimal and there is a need for the creation of a "joint mechanism for integration of technological and intelligence capabilities" (Dagoni 2015).

Israel can look to improve its cyber-regulatory environment at the governmental and private levels by more clearly defining who the regulator is. Currently, there is no regulation for business and civilian sectors, and it remains unclear who should have such authority. The attempt to have different sectorial regulators may lead to different levels of cybersecurity requirements from various sectors, including energy, health, communications, food production, and others. The NCB is the organization that is best suited to such a task. Because of its remit, it already has access to relevant information, is currently engaged in helping to create such regulations, and has extensive ties to private companies and organizations.

Technology alone, however, will likely not be able to solve cybersecurity dilemmas. Israel must utilize regular intelligence means in the physical world. Intelligence about state, nonstate, and individual actors is just as critical for early warning in the cyber realm as it is in the physical realm. Israel is currently moving many intelligence resources into the cyber world, but not everything important is said online (Siboni 2014).

Despite Israel's advanced cyber defenses, eventually an attack will succeed in causing damage. The question then is how it—or any state—recovers. Israel should develop clear plans and guidelines for what actions to take in such a situation. The effort to design such a plan should also include which networks are most important to protect. When designing networks, Israel could craft legislation that requires that features aimed at improving resilience be built into systems to speed and support the recovery process. There are situations where physical overrides should be built in as well. Additionally, building resilience includes creating plans to deal with the possible physical effect of cyberattacks.

The Israeli experience points to a number of vulnerabilities and opportunities the cyber realm presents to any advanced nation. Israel has thus far done well in defending itself and using the vulnerabilities of its opponents to its advantage, but, as noted, there is still room for Israel to improve. The Israeli example can serve to provide ideas for any state looking to improve its utilization of the cyber realm.

References

Aizescu, Sivan. 2014. "Israeli Banks Seek to Set up Joint Cybersecurity Center." Haaretz, May 26. Accessed June 30, 2014. http://www.haaretz.com/business/.premium-1.592767.

Applegate, Scott D. 2012. "The Principle of Maneuver in Cyber Operations." Presented at the Fourth International Conference on Cyber Conflict, Tallinn, Estonia, June 5–8. Accessed June 20, 2014. http://www.ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

Arutz Sheva. 2012. "Report: Bank of Israel Raises Cyber Defenses." Arutz Sheva, February 17. Accessed June 3, 2014. http://www.israelnationalnews.com/News/Flash.aspx/232390#.U8VI7fldVqU.

Baram, Gil. 2013. "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case." *Military and Strategic Affairs* 5: 23–43.

Ben-David, Alon. 2011. "Playing Defense." *Aviation Week and Space Technology* 173: 57.

Bergman, Ronen. 2012. "Shin Bet Allows Sneak Peek at New Cyber Warfare Unit." Ynetnews, December 12. Accessed July 20, 2014. http://www.ynetnews.com/articles/0,7340,L-4322499,00.html.

Bob, Yonah Jeremy. 2013. "Rule of Law: Obama, Israel and Cyber Warfare." Jerusalem Post, March 22. Accessed June 15, 2014. http://www.jpost.com/Features/Front-Lines/The-cyber-partys-over-307367.

Carr, Jeffrey. 2012. *Inside Cyber Warfare.* Cambridge: O'Reilly.

Clarke, Richard A. 2008. *Your Government Failed You.* New York: Harper Collins Publishers.

Clarke, Richard A., and Robert K. Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco, HarperCollins Publishers.

Cohen, Gili. 2013. "IDF Doubled its Defenses against Cyber Attacks." Haaretz (Hebrew), January 9. Accessed July 25, 2014. http://haaretz.ubik.net/news/politics/1.1902961.

Dagoni, Rennes. 2015. "Yadlin: Cyber Warfare, a Country Must Attack, Not Just Defend." Globes.co.il, April 29. Accessed April 30, 2015. http://www.globes.co.il/news/article.aspx?did=1001031543.

Demchak, Chris C. 2011. *Wars of Disruption and Resilience.* Athens: University of Georgia Press.

Dvorin, Tova. 2014. "Secret Shin Bet Unit at the Front Lines of Israel's Cyber-War." Arutz Sheva, April 25. Accessed July 25, 2014. http://www.israelnationalnews.com/News/News.aspx/179925#.U7b-P_ldVqU.

Economist. 2014. "A is for Algorithm." The Economist, April 26. Accessed April 28, 2014.

Efrati, Rami, and Lior Yafe. 2012. "The Challenges and Opportunities of National Cyber Defense." Israel Defense, August 11. Accessed June 30, 2014. http://www.israeldefense.com/?CategoryID=512&ArticleID=1557.

Egozi, Arie. 2011. "The Secret Cyber War." *Military Technology* 35: 5–6.

Eisenstadt, Michael, and David Pollock. 2012. "Asset Test: How the United States Benefits from Its Alliance with Israel." *Washington Institute for Near East Policy, Strategic Reports* 7: 1–60.

Elran, Meir, and Gabi Siboni. 2015. "Establishing an IDF Cyber Command." Institute for National Security Studies 719: 1–3. Accessed July 8, 2015. http://www.inss.org.il/index.aspx?id=4538&articleid=10007.

Even, Shmuel, and David Siman-Tov. 2012. "Cyber Warfare: Concepts and Strategic Trends." Institute for National Security Studies 179: 1–95. Accessed June 12, 2014. http://www.inss.org.il/uploadimages/Import/%28FILE%291337837176.pdf.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53: 23–40.

Farwell, James P., and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival* 54: 107–20.

Fulghum, David. 2010. "No Fingerprints." *Aviation Week and Space Technology* 172: 29–30.

Fulghum, David. 2012. "Bombing Iran." *Aviation Week and Space Technology* 174: 29.

Grauman, Brigid. 2012. "Cyber-security: The Vexed Question of Global Rules." Security and Defense Agenda, pp. 1–104. Accessed January 7, 2014. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=139895.

Harel, Amos. 2012. "The IDF is Preparing for War in Cyberspace." Haaretz (Hebrew), September 25. http://www.haaretz.co.il/news/politics/1.1830427.

Hathaway, Ooona, Rebecca Crootof, Philip Levitz, and Haley Nix. 2012. "The Law of Cyber-Attack." *California Law Review* 100: 817–5.

Herzallah, Mohammed J. 2009. "Israel Fights Wire with Wire." Newsweek, July 27, 11.

Hiner, Jason. 2013. "How Israel is Rewriting the Future of Cybersecurity and Creating the Next Silicon Valley." Tech Republic. Accessed May 15, 2014. http://www.techrepublic.com/article/how-israel-is-rewriting-the-future-of-cybersecurity-and-creating-the-next-silicon-valley/#.

Hirshoga, Or, and Nati Toker. 2012. "Cyber Battles against Israel." The Marker (Hebrew), November 22. Accessed June 30, 2014. http://www.themarker.com/technation/1.1871058.

Institute for National Security Studies, and The Cyber Security Forum Initiative. 2014. "Cyber Intelligence Report—July 15, 2014." Defense Update, July 15. Accessed July 16, 2014. http://defense-update.com/20140715_cyber-intelligence-report-july-15-2014.html.

Israel Ministry of Foreign Affairs. 2013. "Deputy FM Elkin: Israel's Cyber Security." Address to the Seoul Conference on Cyberspace 2013, October 16. Accessed July 29, 2014. http://mfa.gov.il/MFA/PressRoom/2013/Pages/Deputy-FM-Elkin-Israel's-Cyber-Security-16-Oct-2013.aspx.

Jerusalem Post. 2013. "Netanyahu: We're Building a Digital Iron Dome." Jerusalem Post, January 1. Accessed May 30, 2014. http://www.jpost.com/Diplomacy-and-Politics/Netanyahu-Were-building-a-digital-Iron-Dome.

Joint Advanced Warfighting School. 2014. *Nothing New under the Sun: Benefiting from the Great Lessons of History to Develop a Coherent Cyberspace Deterrence Strategy.* Lexington, KY: CreateSpace Independent Publishing Platform.

Katz, Yaakov. 2012a. "Barak: Israel Seeks to be Global Cyber Leader." Jerusalem Post, June 6. Accessed July 30, 2014. http://www.jpost.com/Defense/Barak-Israel-seeks-to-be-global-cyber-leader.

Katz, Yaakov. 2012b. "Elb Unveils New Cyber War Simulator." Jerusalem Post, May 6. Accessed July 30, 2014. http://www.jpost.com/Defense/Elbit-unveils-new-cyber-war-simulator.

Katz, Yaakov. 2012c. "Security and Defense: Israel's Cyber Ambiguity." Jerusalem Post, May 31. Accessed July 30, 2014. http://www.jpost.com/Features/Front-Lines/Security-and-Defense-Israels-Cyber-Ambiguity.

Khazan, Olga. 2012. "Anonymous Is Hacking Israeli Web Sites." Washington Post, November 17. Accessed July 30, 2014. http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/17/anonymous-is-hacking-israeli-web-sites/.

Lappin, Yaakov. 2013a. "Cyber-Terrorism: Defending the Country's Online Borders." Jerusalem Post, February 5. Accessed June 15, 2013. http://www.jpost.com/Features/Front-Lines/Cyber-terrorism-Defending-the-countrys-online-borders.

Lappin, Yaakov. 2013b. "Military Affairs: The IDF's Silent Attack Force." Jerusalem Post, May 11. Accessed June 15, 2013. http://www.jpost.com/Features/Front-Lines/Military-Affairs-The-silent-attack-force-312716.

Lappin, Yaakov. 2014a. "IAI Opens Cyber R&D Center in Singapore." Jerusalem Post, February 13. Accessed June 25, 2014. http://www.jpost.com/Defense/IAI-opens-cyber-R-and-D-center-in-Singapore-341294.

Lappin, Yaakov. 2014b. "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says." Jerusalem Post, August 17. Accessed June 25, 2014. http://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339.

Levi, Ram. 2011. "The Fifth Fighting Space." Israel Defense, December 16. Accessed June 25, 2014. http://www.israeldefense.com/?CategoryID=512&ArticleID=706.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Arlington, VA: Rand Corporation—Project Air Force.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22: 365–404.

Mandiant. 2014. "M-Trends 2014: Beyond the Breach." FireEye. Accessed November 30, 2014. https://www.mandiant.com/resources/mandiant-reports/.

Moore, Jack. 2015. "Anonymous's 'Electronic Holocaust' Against Israel Falls Flat." Newsweek.com, April 7. Accessed April 8, 2015. http://europe.newsweek.com/anonymous-electronic-holocaust-against-israel-has-limited-success-320176.

National Cyber Bureau. 2014. "Mission of the Bureau." *The National Cyber Bureau—Office of the Israeli Prime Minister*. Accessed 8, 2014. http://www.pmo.gov.il/english/primeministersoffice/divisionsandauthorities/cyber/pages/default.aspx.

Nye, Joseph S. Jr. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5: 18–38.

Opall-Rome, Barbara. 2015. "Israel to Consolidate Cyber Spending, Ops." DefenseNews.com, June 21. Accessed June 22, 2015. http://www.defensenews.com/story/breaking-news/2015/06/18/israel-establish-cyber-command-integrate-c4i-defensive-offensive/28916147/.

Parmenter, Robert C. 2013. "The Evolution of Preemptive Strikes in Israeli Operational Planning and Future Implications for Cyber Domain." School of Advanced Military Studies at the United States Army Command and General Staff College, Fort Leavenworth, KS: US Army Command and General Staff College, May 23: 1–68.

Perlroth, Nicole. 2014. "Cyberespionage Attacks Tied to Hackers in Iran." The New York Times, May 29. Accessed June 1, 2014. http://bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/?_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&partner=rssnyt&emc=rss&_r=2.

Pfeffer, Anshel. 2009. "Israel Suffered Major Cyber Attack During Gaza Offensive." Haaretz, June 15. Accessed June 1, 2014. http://www.haaretz.com/news/israel-suffered-massive-cyber-attack-during-gaza-offensive-1.278094.

Prime Minister's Office. 2014. "Moving the ICT from the Finance Ministry to the Prime Minister's Office." Prime Minister's Office (Hebrew). Accessed December 25, 2014. http://www.pmo.gov.il/Secretary/GovDecisions/2014/Pages/dec2099.aspx.

Rapaport, Amir. 2014. "ISA in the Cyber Era: An Inside Look." IsraelDefense.Co.Il, September 5. Accessed December 1, 2014. http://www.israeldefense.co.il/en/content/isa-cyber-era-inside-look.

Ravid, Barak. 2011. "Netanyahu Formed a Team to Prepare for Israeli Attacks on Computer Networks." Haaretz (Hebrew), April 3. Accessed June 20, 2014. http://www.haaretz.co.il/captain/software/1.1170180.

Ravid, Barak. 2014a. "Battle Move in Israel's Turf War: Shin Bet Loses Authority Over 'Civilian Space'." Haaretz, September 21. Accessed October 7, 2014. http://www.haaretz.com/news/national/1.616990.

Ravid, Barak. 2014b. "Israeli Security Agencies in Turf Battle over Cyber War: Netanyahu to Decide." Haaretz, September 14. Accessed October 1, 2014. http://www.haaretz.com/news/diplomacy-defense/1.615637.

Reuters. 2013. "Iran Ups Cyber Attacks on Israeli Computers: Netanyahu." Reuters, June 9. Accessed June 2, 2014. http://www.reuters.com/article/2013/06/09/us-israel-iran-cyber-idUSBRE95808H20130609.

Rid, Thomas, and Peter McBurney. 2012. "Cyber Weapons." *RUSI Journal* 157: 6–13.

Ruble, Kayla. 2014. "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak." Vice.com, July 7. Accessed July 9, 2014. https://news.vice.com/article/syrian-hackers-hijack-idf-twitter-sparking-fears-of-nuclear-leak.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Crown.

Shackle, Samira. 2012. "Cyber Warfare Is Key Priority for Israel." Middle East Monitor, November 2. Accessed June 8, 2014. https://www.middleeastmonitor.com/blogs/politics/4546-cyber-warfare-is-key-priority-for-israel.

Shamah, David. 2014. "Hackers Threaten 'Israhell' Cyber-Attack over Gaza." The Times of Israel, July 9. Accessed July 10, 2014. http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza/.

Siboni, Gabi. 2014. "Cyber-tools are No Substitute for Human Intelligence." Haaretz, July 2. Accessed July 2, 2014. http://www.haaretz.com/opinion/.premium-1.602413#.

Siboni, Gabi, and Ofer Assaf. 2015. "Guidelines for Israel's National Strategy in Cyberspace." *Institute for National Security Studies* (Hebrew), Memoranda 149. Accessed October 30, 2015. http://www.inss.org.il/uploadImages/systemFiles/memo149.pdf.

Silber, Jonathan. 2012. "Cyber Vandalism—Not Warfare." Ynetnews.com, January 26. Accessed June 20, 2014. http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

Silverstein, Richard. 2012. "IDF to Double Unit 8200 Cyber War Manpower." richardsilverstein.com, October 23. Accessed June 30, 2014. http://www.richardsilverstein.com/2012/10/23/idf-to-double-unit-8200-cyber-war-manpower/.

Singer, Peter W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

Sklerov, Matthew J. 2012. "Responding to International Cyber Attacks as Acts of War." In *Inside Cyber Warfare*, edited by Jeffery Carr, 45–76. Cambridge: O'Reilly.

Soffer, Ari. 2014. "Security Services 'Foiled Massive Cyber-Attack on Israel.'" Arutz Sheva, August 28. Accessed August 30, 2014. http://www.israelnationalnews.com/News/News.aspx/184518#.U_ACmNm7Wg.

Steinherz, Tal. 2014. "Israeli Innovation in Cyber-Technology." Presentation to the Herzliya Conference, Herzliya, Israel, June 9.

Supervisor of Banks. 2015. "On Cyber Defense Management." Proper Conduct of Banking Business Directive—361—Israeli Government. Accessed May 8, 2015. http://www.bankisrael.gov.il/en/BankingSupervision/SupervisorsDirectives/ProperConductOfBankingBusinessRegulations/361_et.pdf.

Times of Israel. 2015. "Rocket Siren Sounds across Country in Ongoing Drill." June 2. Accessed June 2, 2015. http://www.timesofisrael.com/rocket-sirens-sound-across-country-in-civil-defense-drill/.

United Press International (UPI). 2012. "Unit 8200 and Israel's High-tech Whiz Kids." June 4. Accessed August 25, 2014. http://www.upi.com/Business_News/Security-Industry/2012/06/04/Unit-8200-and-Israels-high-tech-whiz-kids/UPI-43661338833765/.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford: Oxford University Press.

Vincent, James. 2014. "Schematics from Israel's Iron Dome Missile Shield 'Hacked' by Chinese, Says Report." The Independent, July 29. Accessed July 30, 2014. http://www.independent.co.uk/life-style/gadgets-and-tech/israels-iron-dome-missile-shield-hacked-by-chinese-military-hackers-says-report-9635619.html.

Winer, Stuart. 2014. "Iranians Launched Cyber-Attack on Israel during Gaza Op." The Times of Israel, August 17. Accessed August 17, 2014. http://www.timesofisrael.com/iranian-cyber-attack-on-israel-during-gaza-op/.

Ynetnews. 2012. "IDF says 'Defined Essence of Cyber Warfare'." Ynetnews, June 4. Accessed August 30, 2014. http://www.ynetnews.com/articles/0,7340,L-4238156,00.htm.

Zetter, Kim. 2012. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers." WIRED, May 28. Accessed March 3, 2015. http://www.wired.com/2012/05/flame/.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown.

Zippori, Michal. 2012. "Hackers Attack Two IsrZivaeli Websites." CNN, January 26. Accessed June 30, 2014. http://www.cnn.com/2012/01/16/world/meast/israel-hacking-attack/.

Zitun, Yoav. 2012. "NCC Holds First Cyber Terror Drill." Ynetnews, Jan 25. Accessed July 30, 2014. http://www.ynetnews.com/articles/0,7340,L-4180485,00.html.

Ziv, Amitai. 2014. "Theft, Business Espionage, and War: Cyber Threats are Good News for High Tech." The Marker (Hebrew), September 14. Accessed September 17, 2014. http://www.themarker.com/technation/1.2432479.