A HOOVER INSTITUTION ESSAY

Persistent Aggrandizement? Israel's Cyber Defense Architecture

ELENA CHACHKO

Aegis Series Paper No. 2002

Introduction

Defend Forward has emerged as a key pillar of current US cyber defense strategy. According to the 2018 Command Vision of the US Cyber Command (CYBERCOM), the concept means that the United States will "defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage."[1] In other words, under Defend Forward, the United States will engage in cyber defense outside US networks and on foreign territory. It will take the initiative instead of waiting for threats to materialize at home.

A related yet distinct operational concept in CYBERCOM's strategic vision is Persistent Engagement. The vision states that:

> Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how we operate—maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate—globally, as close as possible to adversaries and their operations. It describes when we operate—continuously, shaping the battlespace. It describes why we operate—to create operational advantage for us while denying the same to our adversaries.[2]

This paper compares these core elements of the US cyber defense strategy with Israel's cyber defense architecture and recent reforms. Since 2011, the Israeli government has worked to centralize and streamline cybersecurity authorities and responsibilities. It has established a new civilian national security agency—the National Cyber Directorate—to oversee cybersecurity preparedness in both the government and the private sector, and to monitor and respond to cyber threats. The government has also drafted advanced, comprehensive cyber legislation in broad consultation with relevant stakeholders from within government, as well as private sector and civil society actors. Importantly, these reforms only extend to domestic cyber defense. Cyber action focusing on foreign targets outside Israeli territory has remained shielded from these reforms.

Substantively, Israel's cyber defense reforms echo the US concept of Persistent Engagement in recognizing the need for continuous monitoring of cyber vulnerabilities and threats. Like US decision makers, the Israeli government has highlighted the necessity of responding to

such threats in an assertive and timely manner. A key difference, however, is that the Israeli approach to cyber defense envisions and invites government monitoring of and operations on *domestic* civilian networks. Moreover, it co-opts the private sector for that purpose.

Israel's cyber defense architecture and operational approach also share similarities with Defend Forward. While recent reforms have avoided regulation of cyber action on foreign territory, Israel has earned a reputation for being a major actor in the realm of international cyber action—both offensive and defensive.[3]

What follows compares the two national strategies. Before turning to the comparison, the paper surveys the major components of the Israeli reforms. The final part of the paper briefly evaluates the Israeli reforms. It considers the trade-offs that the Israeli reforms make between the role of the government and that of the private sector, and between operational effectiveness and civil liberties. It argues that the trajectory of the Israeli reforms is best described as persistent aggrandizement on the government's part, at the expense of the private sector and privacy.

Israel's Cyber Defense Reform

Government Resolutions 3611 and 2444

Beginning in 2011, Israel's government adopted a series of resolutions to overhaul cyber defense authorities and create new national cybersecurity organs. These resolutions are the equivalent of executive directives issued by government ministers without parliamentary approval (this paper uses the term "government" to refer to the Israeli executive branch—government ministers and the administrative state—excluding parliament). Resolution 3611, adopted in August 2011, provided that the government would work toward advancing national cyber capabilities, strengthening protection of critical national infrastructure, and regulating powers and responsibilities in the cyber realm.[4]

In addition, the resolution approved the establishment of the National Cyber Bureau in the prime minister's office with wide-ranging cybersecurity responsibilities. The bureau was tasked with advising the government on cyber policy issues and coordinating policy across government, among other assignments. It was also responsible for facilitating cooperation among relevant stakeholders, including academia and the private sector, as well as government ministries and existing national security agencies: the Israel Defense Forces (IDF—the country's military); the Israeli Security Agency (ISA—the internal security service, colloquially known as Shabak); the Mossad intelligence agency; the police force; and the Director of Security of the Defense Establishment, a unit within the Defense Ministry.

Subsequently, in 2015, the government adopted Resolution 2444, which approved the establishment of another centralized cybersecurity organ—the National Cyber Defense Authority.[5] Resolution 2444 envisioned that the authority would operate side by side with

the bureau in the prime minister's office. It shifted the focus of the bureau's responsibilities from operations to strategic planning and capacity building.

Resolution 2444 entrusted the authority with operational responsibility for preventing cyberattacks and addressing threats in real time in cooperation with other national security agencies. The resolution further provided that the authority would serve as a focal point for cyber-related intelligence and analysis, work to increase readiness to thwart cyberattacks across different sectors, issue guidelines, regulate cybersecurity services, and guide the work of cybersecurity units within government ministries.[6]

Furthermore, the authority was tasked with establishing a Cyber Emergency Response Team (CERT) that would service stakeholders across the economy. According to Resolution 2444, the national CERT would provide assistance in cyber defense, facilitate information sharing, and allow for coordination between security agencies and other actors.

Resolution 2444 only defined the structure and powers of the authority in general terms. It created many spaces of potential friction among the actors involved in cybersecurity policy and operations, and tasked different organs with seemingly overlapping responsibilities.

A key example of these ambiguities was the resolution's treatment of the relationship between the authority and the ISA. While section 12 of Resolution 2444 made it clear that the resolution did not detract from the cyber-related statutory authorities of the ISA, section 9 invited the bureau to put forward a plan for the transfer of responsibility for cyber defense of critical computer infrastructure from the ISA to the authority through the amendment of the Regulation of Security in Public Bodies Law, 1998. As part of the implementation of Resolution 2444, in August 2016, the Israeli parliament (Knesset) passed a temporary amendment to the Regulation of Security in Public Bodies Law to facilitate the transfer of responsibility in this area from the ISA to the authority.[7]

This amendment only addressed one aspect of the authority's operations. At the time of its adoption, work was already underway at the Israeli Ministry of Justice and the bureau on comprehensive legislation that would regulate the authority's powers and responsibilities, as well as other cyber defense matters.[8]

The authority began operating in 2016, and the CERT was up and running by 2017. The CERT includes a National Incident Management Center, which works around the clock and handles reports on cyberattacks, vulnerabilities, and security breaches across the Israeli economy.[9] The center also facilitates information sharing on cyberattacks and threats. It operates under a set of "action principles" issued by the prime minister's office in coordination with Israel's attorney general.[10] In 2018, the authority and the CERT were merged with the bureau under the new National Cyber Directorate, due in part to overlapping authority and bureaucratic redundancies between the bureau and the authority under the original framework.[11]

The IDF also set cyber reforms in motion in parallel to the reforms on the civilian end. In June 2015, Lt. Gen. Gadi Eisenkot, then the chief of staff of the IDF, decided to create a unified cyber command that would take the lead on cyber readiness within the military.[12] Prior to that decision, the Telecommunications Directorate of the IDF was responsible for cyber defense within the military, while the Israeli equivalent to the NSA, the signals intelligence unit of the Directorate of Military Intelligence (DMI), was responsible for intelligence collection and foreign cyber operations.[13]

However, in early 2017, this ambitious plan was abandoned in favor of a more careful approach that largely preserved the previous organizational division of labor between the DMI and the Telecommunications Directorate.[14] The reason for the change of direction was reportedly fear that a unified cyber command might harm the intelligence collection and foreign cyber work of the DMI.[15]

Legislative Reform

Guiding principles In parallel to the continuous development of new executive organs and authorities in the area of cyber defense, the government has advanced comprehensive legislation to enshrine these reforms in statute. In June 2018, the prime minister's office released a draft Cyber Defense and National Cyber Directorate Bill.[16] The legislative effort has not advanced beyond the draft stage because Israel's year-and-a-half-long political stalemate, followed by the COVID-19 crisis, caused major legislative efforts to grind to a halt. Parliament has yet to take up the bill. Still, the Israeli government is likely to advance it. Cyber reform has long been a priority of Prime Minister Benjamin Netanyahu, who has vowed to make Israel "one of the five global cyber superpowers."[17]

The draft reflects the three key policy principles that have ostensibly guided executive reform efforts to date: the need for a concerted national response, facilitating cooperation between government and the private sector, and preserving the authorities and responsibilities of the "old" national security establishment.

First, according to the explanatory remarks attached to the draft, the bill is guided by the assumption that addressing cyber threats requires a coordinated, national effort. The remarks point out that cyber threats can originate anywhere in the world, do not respect physical boundaries, allow attackers anonymity, and are capable of causing significant harm to the national economy, critical infrastructure, and human lives.

Second, the bill underscores that cyberspace is a predominantly civilian space. Civilian organizations possess most of the relevant information for identifying threats to their networks. They also control key tools for addressing such threats. The bill therefore places ultimate responsibility for network defense (excluding, of course, military and other security establishment networks) with civilian organizations and individuals. At the same time, the bill recognizes that civilian organizations cannot defend themselves alone in light of the

scope of potential threats, the need for expertise in order to combat them, and the narrow perspective of individual organizations. Effective defense, it concludes, requires cooperation between the government and the private sector.

Finally, the draft bill states that "the proposed bill is not designed to change the purpose or authorities of additional bodies that operate in Israeli cyberspace under applicable legal frameworks, including the ISA."[18] Given the broad, ill-defined authorities of the national security establishment in the cyber realm (described in greater detail in Part II), vesting the operational responsibility to prevent and address cyber threats at home in the new Cyber Directorate was bound to draw the ire of the security establishment, especially the ISA, and invite turf wars. Unlike the IDF and Mossad, whose operations are geared toward foreign threats, the ISA has certain domestic security responsibilities. Conflicts between the newly established civilian cybersecurity organs and the national security establishment have accordingly plagued the legislative effort.

An August 2016 report by the Knesset Cyber Defense subcommittee described conflict and lack of cooperation between the new Cyber Authority (later the "Directorate") and the security establishment. It noted some improvement in cooperation after the signing of a Memorandum of Understanding between the ISA and the authority in June 2016. The report also predicted that there would be no avoiding at least some chipping away at ISA prerogatives with the entry of a new actor, the authority, into the cyber field, notwithstanding Resolution 2444's explicit guarantee that the power of the ISA would be preserved.[19]

Disagreements over the scope and content of the legislation came to a head in 2017, with the publication of a letter from the leaders of the major Israeli security agencies to the prime minister and his security cabinet. The security agencies expressed their strong objection to a draft presented to them by the bureau. The letter stated that the draft legislation ignored the existing authorities of the security agencies and the government resolutions pertaining to cybersecurity that explicitly excluded the security establishment from their purview. The letter further stated that by granting the Cyber Authority expansive powers without clearly defining its purpose, the draft could severely harm the work of the security community in the cyber realm. The letter concluded with a call to scrap the draft and negotiate a new one that would take account of the position of the security agencies.[20]

We do not know how these conflicts were eventually resolved. We do know, however, that the security establishment has been highly successful in defending its cyber equities in the framework of the new reform, as evidenced by the draft bill's explicit commitment to leave those equities undisturbed. This means that the national security establishment will generally maintain whatever domestic cyber authorities it had and avoid new restrictions on its foreign operations.

The cyber defense chapter The proposed bill consists of three main chapters: an organizational chapter, which outlines the responsibilities of the National Cyber Directorate

and its structure; a cyber defense chapter, which addresses authorities related to detection and defense against cyber threats; and a regulatory chapter, which includes provisions for improving the cybersecurity preparedness of the Israeli economy. Here I focus on the cyber defense chapter.

That chapter addresses the operational aspects of preventing, identifying, and containing cyberattacks that impact civilian organizations, a category that includes both public entities and private sector actors. The bill conceives of a "cyberattack" as an act falling within "the range of actions that constitute abuse of a computer or computerized information by computational means." Section 1 more specifically defines the term as "activity designed to impair use of a computer or computational material stored therein," and includes a non-exhaustive list of more specific circumstances meeting this criterion.[21]

The operational authorities that the bill grants the directorate can roughly be divided into two categories: (1) information collection, analysis, and dissemination and (2) direction and intervention.

Information collection, analysis, and dissemination The bill empowers the Cyber Directorate to collect and analyze incident information, as well as information about vulnerabilities, technologies, attack methods, and tools. The directorate may require any organization—governmental or private—to provide relevant information.[22] Moreover, the bill authorizes the directorate to enter premises where cybersecurity information necessary for addressing cyberattacks is believed to be located and requires the directorate to share cybersecurity information with all relevant stakeholders.[23]

"Cybersecurity information" is defined broadly as "information that could help detect, address or prevent a cyberattack," including information about vulnerabilities, malware, and attack methods as well as information about response methods. The bill restricts collection of information about identifiable individuals or organizations and limits use of any information collected to cyber defense purposes—not law enforcement or general intelligence collection. It establishes rules for handling information collected from civilian entities and preventing abuse, and it creates both internal and semi-independent oversight and privacy protection mechanisms.

One of the most potentially intrusive features of the bill from a privacy standpoint is what the bill calls the "Detection and Identification" apparatus. Section 17 directs the directorate to create an apparatus to collect and process cybersecurity information from a non-exhaustive list of entities in real time. This provision implies constant directorate monitoring of the networks of the covered entities. Most of these entities are government ministries and public entities responsible for critical infrastructure, but Section 18(4) also allows for the monitoring of telecommunications companies under certain conditions. Constant government monitoring of telecoms—the arteries of national communication—would invariably create a large opening for government abuse.

Direction and intervention The bill would also authorize the directorate to intervene directly to defend civilian networks. It provides for two main methods of intervention: First, the bill would give the directorate authority to issue binding directives to entities that have been attacked or entities for which there is reason to believe that an attack is forthcoming.[24] Second, the bill would allow the directorate to operate on compromised networks—a more intrusive form of intervention that potentially gives the directorate direct access to the computer networks of private entities. To offset this invasive authority, the bill requires the directorate to obtain consent or a judicial warrant prior to operating on networks, although there is a 24-hour emergency exception to this warrant requirement.[25]

In addition to providing the directorate significant direction and intervention authorities, the bill outlines a standard for the activation of these authorities: the directorate is allowed to step in when a cyberattack has occurred or might occur if a vital national interest is at stake, and the benefit of directorate intervention is proportional to the harm to the attacked organization's operations and affected privacy rights.[26]

Section 1 of the bill defines "vital interest" extremely broadly. The definition extends to national security; public and individual safety; preventing significant risks to public health or the environment; protecting the national economy; ensuring the functioning of essential systems, infrastructure, and organizations that provide significant services; and preventing substantial invasions of privacy. The bill would also empower the prime minister to deploy the directorate to protect any interest that he determines is "vital." In other words, the threshold for directorate intervention in private-sector cybersecurity crises is alarmingly low and easily manipulable.

Notably, the bill emphasizes that the Cyber Directorate is only responsible for identifying, containing, and analyzing cyberattacks at home (i.e., within Israel)—echoing the tension between the newly established Cyber Directorate and the traditional national security establishment. The task of "handling the attacker" falls to "the responsible actors." Presumably the IDF, Mossad, and the ISA would be the actors responsible for handling foreign attackers outside Israel's territory.[27]

In addition, Section 71 of the bill allows the ISA to assume the directorate's powers when a cybersecurity threat is related to counterterrorism or espionage. In other words, the bill would augment the ISA's existing authorities to operate on domestic networks by allowing the agency to step into the directorate's shoes. This authorization would provide a significant boost to the domestic authority of a security organ primarily responsible for combating foreign threats.

Israel's Reform and US Strategy

The Israeli cyber defense architecture under these recent reforms echoes the US concepts of Defend Forward and Persistent Engagement. Nevertheless, there are key differences. For one,

Israel's Defend Forward equivalent is even less constrained by domestic law than is its US parallel. Furthermore, the Israeli reforms create a substantial role for government in defending *domestic* networks—including private networks—*within* Israeli territory. The reforms also harness the private sector in ways that the current US strategy does not contemplate.

The Israeli Defend Forward Equivalent

Defend Forward's aim of operating "as close as possible to the origin of adversary activity" implies that it is mainly geared toward external action—action outside of US networks, often outside US territory. It may involve offensive action designed to harm adversary networks and infrastructure, as well as essentially defensive measures to neutralize or thwart ongoing or expected adversary operations.

The direct Israeli equivalent to this category of operations is the cyber-related work of the traditional national security establishment—mainly the IDF, Mossad, and the ISA. Although much is unknown about the nature and scope of their activities, these agencies reportedly carry out cyber operations against foreign adversaries outside Israeli networks and territory. Famous examples include Israel's role in the Stuxnet attack on Iran's nuclear facilities, as well as a recent cyberattack, attributed to Israel, designed to disrupt the operations of an Iranian port in response to an Iranian attack on Israeli water infrastructure. The roles and authorities of Israel's national security agencies in this area have largely remained untouched by the Israeli cyber defense reform described in Part I, which focuses on domestic cyber defense.

Section 5 of Resolution 3611 explicitly excluded national security agencies from the resolution's purview. The resolution only noted that national security agencies would be subject to special arrangements mutually agreed upon with the new cyber defense agency (now the National Cyber Directorate). Subsequent resolutions, including Resolution 2444, also excluded or otherwise exempted the national security establishment from their scope, reaffirming—with narrow exceptions—that the reform did not aim to detract from any of the establishment's existing cyber authorities and responsibilities. As we have seen, the draft cyber bill likewise adopted this stance.

The exceptions for national security agencies in Israel's new domestic cyber defense regulatory scheme have created a bifurcated regime. Reform efforts have focused on domestic cyber defense regulation and established new institutions for that purpose, while the cyber work of the old national security establishment—domestic and foreign—has been allowed to continue largely under preexisting parameters. As a result, the virtually nonexistent domestic legal regime that applies to these agencies continues to govern their cybersecurity operations, especially when they act against foreign targets.

To appreciate just how rudimentary the domestic legal regime governing the operations of Israel's national security establishment is, consider Basic Law: The Military—which defines the authority of the vast and powerful IDF, subordinates it to civilian control of the government,

and imposes mandatory service obligations. This fundamental constitutional norm consists of a grand total of six one-sentence paragraphs.[28] There is no statute that governs the work of the Mossad. The Knesset painstakingly passed an ISA Law in 2002, but even this law consists of broad and ambiguous language and says very little about the ISA's specific operational authorities.[29]

Generally, the foreign affairs and national security powers of the Israeli government are deemed residual authorities, that is, discretionary executive powers that do not depend on explicit constitutional or statutory grants of authority. These are powers that the government may wield unless there is a conflicting statute, or the action in question violates constitutional rights.[30]

On the sub-constitutional level, there exist statutes that restrict unauthorized access by any actor to computer networks and impose civil and criminal penalties for violations. Other legislation governs data handling.[31] However, these statutes only apply to the domestic operations of the national security agencies (to the extent that they have authority to carry out domestic operations).[32] They do not cover external cyber action or foreign intelligence collection.

Consequently, very little is known about the legal and policy frameworks that govern the cyber work of the IDF, Mossad, and the ISA outside Israeli territory. That framework consists of inscrutable classified internal orders, guidelines, and regulations.

The rudimentary legal framework that applies to the Israeli national security establishment's operations abroad is thus far less robust than the regime that applies to similar operations in the United States. Israel lacks a detailed constitutional framework to govern international use of force, much less action that falls below the use of force threshold—the type of action Defend Forward appears to encompass. There is no parallel to the War Powers Resolution, nor is there a tradition of publishing detailed executive branch legal opinions about the legality of various uses of force abroad (flawed and permissive as they may be).

Furthermore, Israeli national security establishment cyber operations on foreign territory are not regulated by statute. By contrast, the US statutory scheme governing this area includes the general legal requirements of Titles 10 and 50 of the United States Code, as well as cyber-specific reforms introduced in recent years through the National Defense Authorization Act. Robert Chesney offers a detailed overview of these legal authorities, which I will not repeat here.[33] He observes: "[t]he domestic legal framework for military cyber operations is surprisingly robust, considering its recent vintage. . . . Congress has responded to the maturation of USCYBERCOM by adopting relatively detailed rules of authorization, process, and transparency."[34]

In sum, Israel's cyber defense approach has operational elements similar to those that inform the US Defend Forward strategy. In contrast to the relatively robust legal regime that applies in the United States in this area, however, Israel's cyber activity abroad remains a legal black hole.

Israel's Persistent Engagement—At Home

The Israeli approach to cyber defense reflects the same threat perception and basic operational approach as does that of the United States. Its guiding principles are essentially similar to what Persistent Engagement calls for: continuous monitoring of global cyber threats to the homeland and determined and timely action. Like the US approach, the Israeli approach to Persistent Engagement also underscores the need for a whole-of-government response to cyber threats.[35]

However, the Israeli framework goes much further than does that of the United States in granting the government invasive cyber defense authorities *at home*. It also imposes a wide range of cybersecurity obligations on the private sector. For example, the new National Cyber Directorate is empowered to collect, synthesize, and disseminate cybersecurity information to and from private entities, including information about their vulnerabilities and other potentially sensitive or proprietary information. It also has authority to step in and direct the responses of private entities to actual or impending cyberattacks. Still more, under the proposed cyber bill, the National Cyber Directorate will be allowed to operate directly on the networks of private actors to contain cyberattacks—even without their consent. The proposed "Detection and Identification" apparatus would involve mass data collection by the directorate on a regular basis, and possibly even monitoring of domestic telecom networks.

The rough parallels to these authorities in the United States can be found in the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Cybersecurity and Infrastructure Security Agency Act of 2018 (CISAA 2018).[36] CISA 2015 encourages companies to *voluntarily* share information about cyber threat indicators and related defensive measures by granting them certain protections for such disclosure. But it does not compel disclosure. CISAA 2018 reorganized the Department of Homeland Security by creating the Cybersecurity and Infrastructure Agency. The functions of this agency appear to be similar in some respects to those of the Israeli National Cyber Directorate. But the Cybersecurity and Infrastructure Agency's authority over the private sector is far more constrained than that of its Israeli counterpart.

Section 2202 of CISAA 2018 outlines the cybersecurity authorities of the secretary of Homeland Security. These authorities include authorization to coordinate various aspects of cyber policy with the private sector and to synthesize information originating in the private sector.

For example, the secretary is authorized to "access, receive, and analyze law enforcement information, intelligence information, and other information from federal government agencies, state, local, tribal, and territorial government agencies, including law enforcement agencies, and *private sector entities*, and to integrate that information" in order to counter terrorist threats. She is also authorized to "recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other

federal government agencies, including sector-specific agencies, and in cooperation with state, local, tribal, and territorial government agencies and authorities, *the private sector*, and other entities" and to "consult with state, local, tribal, and territorial government agencies and *private sector* entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States."

Yet, CISAA 2018 does not authorize the secretary to issue binding directives to private actors in the event of a cyberattack or threat thereof. And the act certainly does not allow the Cybersecurity and Infrastructure Agency to step in and operate directly on the networks of affected private actors without their consent. Moreover, many of the secretary's authorities in Section 2202 are limited by the objective of detecting and responding to terrorist threats. The Israeli cyber bill lacks a similar subject-matter constraint. As previously mentioned, the bill's standard for the activation of the National Cyber Directorate's direction and intervention authorities, the "vital interest" standard, is extremely broad and open to interpretation.

It may be that granting the government sweeping powers to direct and manage the containment of cyberattacks in the private sector is operationally necessary to defend against cyber threats effectively. That certainty appears to be the position of the Israeli government. We lack the tools to assess the operational necessity of these measures or their efficacy because relatively little is publicly known about the cyber threat landscape, how Israel has responded in practice in every instance, whether its responses achieved the desired outcomes, and whether coercion of private actors (as opposed to voluntary cooperation) was actually needed.

Since its inception, the new Cyber Directorate has advertised a number of instances of successful identification and containment of cyberattacks on civilian Israeli targets, but these examples probably only reveal a small part of the picture.[37] These reports also provide little detail about directorate cooperation with the private sector, related conflicts and obstacles, and the extent to which the directorate had to compel cooperation of private actors.

I leave the operational analysis to others. Instead, the next part considers how the existing and proposed Israeli cyber defense architecture creates openings for government aggrandizement and potential abuse.

Collaboration or Aggrandizement?

At first glance, the government's statements to date and the explanatory remarks attached to the draft cyber bill reflect a collaborative model of responsibility for cyber defense and preparedness between government and the private sector. Israel's new cyber defense bureaucracy and related legal authorities are said to be predicated on the assumption that while the private sector has significant advantages in the area of cyber defense, and every organization should assume primary responsibility for its own security, the nature of the modern cyber threat environment is such that individual organizations cannot operate alone. An active governmental role is therefore essential.

Nevertheless, in practice, Israel's new cybersecurity architecture establishes the National Cyber Directorate as a highly centralized government component with wide-ranging authorities that the proposed legislation would expand even further. Israel's cybersecurity reform ultimately prioritizes the government and exudes government dominance, notwithstanding the rhetoric of private sector empowerment.

The proposed legislation would shift the balance of power between government and the private sector even more in favor of the government. It would undermine the collaborative prong of the regulatory model and create substantial risk of government overreach, politicization, and abuse. Naturally, the directorate's proposed far-reaching powers have drawn criticism from rights advocates and businesses—both local actors and global corporations like Google.[38] Critics have expressed concern over the prospect of government penetration into their networks, centralized synthesis and distribution of information about their vulnerabilities, and the sharing of other proprietary information.

Israel's cybersecurity architecture is particularly susceptible to politicization because the National Cyber Directorate effectively reports directly to the prime minister. The proposed legislation would enshrine the prime minister's broad discretion to expand the directorate's roles and authorities, from cybersecurity defined in the narrow sense of protecting critical computer networks to sanctioning measures that involve substantive intervention in content. While there is an argument to be made in favor of such authorities—for instance, to combat foreign disinformation campaigns for political aims on Israeli networks—the proposed bill would grant the prime minister what amounts to a blank check to make judgments about what constitutes disinformation, among other things.

The expansive powers of the National Cyber Directorate when it comes to domestic cyber defense add to the relative freedom the government enjoys in the area of external cyber action. As we have seen, cyber action against foreign targets, conducted by the military and security agencies like the Mossad and ISA, remains a legal black hole. The operations of these bodies are lightly regulated in primary legislation. Other applicable legal instruments are classified and not subject to public scrutiny.

What is more, the national security establishment has been highly successful at protecting its turf and powers in the process of domestic cybersecurity reform, due in large part to the substantial influence it wields in internal decision making. While the precise division of labor between the National Cyber Directorate and Israel's national security establishment remains unclear, the government has gone to great lengths at every turn to emphasize that the reform does not detract from the cybersecurity powers of the old national security establishment. The ISA in particular appears to have taken advantage of the Cyber Directorate's powers to augment and leverage its own.[39]

What emerges is a combination of broad, ill-defined, and intrusive government authorities in the domestic cybersecurity space, combined with even broader, less regulated government

authority with respect to external cyber action and foreign threats. This outcome militates in favor of imposing meaningful restrictions and oversight—internal, parliamentary, and judicial—on the National Cyber Directorate's powers if the proposed legislation is to move forward. Moreover, it is past time to consider whether granting the national security establishment free rein when it acts outside Israeli territory is consistent with the rule of law in a modern democracy.

Conclusion

Israel's cyber defense architecture shares much with that of the United States and has parallels with both Defend Forward and Persistent Engagement. There are, however, key differences: Israel's Defend Forward component is far less regulated than is its American counterpart. Its Persistent Engagement equivalent also goes much further than does the US approach in giving the government extensive authorities to direct and even take over cyber defense in the private sector.

Israel's cyber defense reform reflects awareness of the challenges involved in effective cyber defense, and an understanding that successfully addressing these challenges requires an economy-wide effort. However, the regulatory balance in this area has shifted too much in favor of the government. This dynamic creates the potential for government aggrandizement, overreach, and abuse. More work is needed to refine the provisions of the proposed cyber bill to eliminate vague and overly broad definitions and authorities and to put in place effective oversight mechanisms—internal, judicial, and parliamentary—to offset these concerns.

NOTES

1 See US Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command 4," 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

2 US Cyber Command, "Achieve and Maintain Cyberspace Superiority," 6.

3 Ronen Bergman and David M. Halbfinger, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks," *New York Times*, May 19, 2020, https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html; William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

4 Government of Israel Resolution No. 3611, Advancing National Capabilities in Cyberspace (August 7, 2011), https://www.gov.il/he/departments/policies/2011_des3611.

5 Government of Israel Resolution No. 2444, Advancing National Preparedness for Cyber Defense (February 15, 2015), https://www.gov.il/he/departments/policies/2015_des2444.

6 See also Government of Israel Resolution No. 2443, Advancing National Regulation and Government Leadership in Cyber Defense, https://www.gov.il/he/Departments/policies/resolution_2443, adopted on the same day as Resolution 2444.

7 Temporary Amendment to the Law Regulating Security in Public Entities, 2016, https://fs.knesset.gov.il/20/law/20_lsr_349197.pdf.

8 See Temporary Amendment to the Law Regulating Security in Public Entities, Part I.B.

9 See Israel National Cyber Directorate, "The Israeli Cyber Emergency Response Team (CERT)," Gov.il, June 5, 2019, https://www.gov.il/en/departments/news/119en.

10 National Cyber Directorate, "National Cyber Emergency Response Team Principles of Operation," Gov.il, retrieved August 17, 2020, https://www.gov.il/BlobFolder/policy/principles/he/principles.pdf.

11 Government of Israel Resolution No. 3270, Merging the Units of the National Cyber Directorate and Related Provisions (December 17, 2017), https://www.gov.il/he/Departments/policies/dec_3270_2017.

12 "IDF to Establish New Cyber Arm," *Times of Israel*, n.d. (2015), retrieved August 17, 2020, http://www.timesofisrael.com/liveblog_entry/idf-to-establish-new-cyber-arm.

13 Meir Elran and Gabi Siboni, "Establishing an IDF Cyber Command," *INSS Insight* No. 719 (July 8, 2015), https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20719%20-%20Meir%20and%20Gabi%20for%20web.pdf.

14 Anna Ahronheim, "IDF Decides Not to Have a Cyber Command Department," *Jerusalem Post*, January 1, 2017, http://www.jpost.com/Israel-News/IDF-decides-not-to-have-a-cyber-command-department-477169.

15 Gili Cohen, "Until a Cyber Arm Is Established: The IDF's Cyber Headquarters Will Be Subordinate to the Telecommunications Directorate," *Haaretz*, January 2, 2017, http://www.haaretz.co.il/news/politics/.premium-1.3193172; Lilach Shoval, "IDF Chief Has Changed His Mind: A Cyber Command Will Not Be Established," *Israel Ha'yom*, January 1, 2017, http://www.israelhayom.co.il/article/440543.

16 The full text of the draft bill is available at Tazkirim.gov.il, https://www.tazkirim.gov.il/s/tzkirim?language=iw&tzkir=a093Y00001RFEcVQAX (hereinafter Draft Bill).

17 Benjamin Netanyahu, "Israel—A Cyber Superpower," *Globes*, April 3, 2016, https://www.globes.co.il/news/article.aspx?did=1001114414.

18 Draft Bill, *supra* note 16, at § 2.

19 The Knesset Foreign Affairs and National Security Committee, Report on the Evaluation of the Distribution of Responsibilities and Authorities With Respect to Cyber Defense in Israel (2016), https://www.knesset.gov.il/committees/heb/docs/bitachon-8-2016.pdf.

20 Jacob Magid, "Security Chiefs Slam Netanyahu over Planned Cyber Defense Body," *Times of Israel*, April 24, 2017, http://www.timesofisrael.com/security-chiefs-slam-netanyahu-over-planned-cyber-defense-body.

21 Such circumstances include, but are not limited to, obstruction of computational operations; deletion or modification of data; unauthorized network penetration or access to information; and obstruction of network communication.

22 Draft Bill, *supra* note 16, at § 20.

23 Draft Bill, *supra* note 16, at § 22 (entering a residence generally requires a judicial order).

24 Draft Bill, *supra* note 16, at § 26.

25 Draft Bill, *supra* note 16, at §§ 27, 32; § 36.

26 Draft Bill, *supra* note 16, at § 1.

27 Draft Bill, *supra* note 16, at § 8, para. 5.

28 Knesset, Basic Law: The Military, 5736–1976, SH 1197 418 (Isr.), https://www.knesset.gov.il/laws/special/eng/basic11_eng.htm.

29 General Security Service Law, 5762–2002, SH 1832 179 (Isr.), https://www.shabak.gov.il/SiteCollectionImages/אודות/shabak-law.pdf.

30 See Knesset, Basic Law: The Government, 5761–2001, SH 1780 158 (Isr.), https://knesset.gov.il/laws/special/eng/basic14_eng.htm, § 32.

31 Amir Cahane and Yuval Shany, "Regulation of Online Surveillance in Israeli Law and Comparative Law," Israel Democracy Institute (2019), https://en.idi.org.il/publications/28246. See, e.g., The Criminal Procedure Law (Enforcement Authorities—Communications Data), 5768–2007, SH 2122 72 (Isr.), https://www.nevo.co.il/law_html/law01/999_876.htm; The Computers Law, 5755–1995, SH 1534 366 (Isr.), https://www.unodc.org/res/cld/document/computer-law_html/Israel_Computers_Law_5755_1995.pdf; The Privacy Protection Law, 5741–1981, LSI 35 136 (1980–81), as amended (Isr.), http://www.nevo.co.il; Secret Monitoring Law, 5739–1979, SH 938 118 (Isr.), https://www.nevo.co.il/law_html/law01/077_001.htm; § 23A, The Criminal Procedure Ordinance (Detention and Search) [New Version], 5729–1969, LSI 2 30 (Isr.). For an overview, see Library of Congress, "Online Privacy Law: Israel," updated July 24, 2020, https://www.loc.gov/law/help/online-privacy-law/2012/israel.php.

32 Save for the police and the ISA, which has certain domestic authorities, national security agencies do not operate domestically.

33 See Robert Chesney, "The Domestic Legal Framework for US Military Cyber Operations," Aegis Series Paper No. 2003, Hoover Institution, July 2020, https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf.

34 Chesney, "The Domestic Legal Framework," 16.

35 US Cyber Command, "Achieve and Maintain Cyberspace Superiority," 4 ("Whole-of-government approaches for protecting, defending, and operating in cyberspace must keep pace with the dynamics of this domain.").

36 Pub. L. No. 114-113, 129 Stat. 2241, 2936 (2015) (codified at 6 U.S.C. §§ 1501–1510 [2018]); Pub. L. No. 115-278, 132 Stat. 4168 (2018) (codified at 6 U.S.C. §§ 651–674 [2018]).

37 Amir Buhbut and Tal Shalev, "Head of the National Cyber Directorate on the Attempted Attack on Water Infrastructure: 'It Could Have Ended in Disaster,'" *WallaNews*, May 28, 2020, https://news.walla.co.il/item/3363509; Udi Ezion and Naomi Zoref, "A Large-Scale Cyber Attack Paralyzed Numerous Israeli Websites: 'Iranian Actors Hacked [the Sites],'" *Calcalist*, May 21, 2020, https://www.calcalist.co.il/internet/articles/0,7340,L-3825453,00.html; Amitay Ziv, "The National Cyber Directorate Thwarted 'A Large Scale Cyber Attack'; the Attackers: Iranian Hackers," *TheMarker*, April 26, 2017, https://www.themarker.com/technation/1.4049930.

38 See, e.g., Comments by Google on the Draft Cyber Defense and National Cyber Directorate Bill, August 28, 2018, https://www.gov.il/BlobFolder/news/cyberlawpublic/he/google.pdf; Comments by the Israel Democracy Institute on the Draft Cyber Defense and National Cyber Directorate Bill, July 11, 2018, https://www.gov.il/BlobFolder/news/cyberlawpublic/he/democracy.pdf; Comments by the Israel Internet Union on the Draft Cyber Defense and National Cyber Directorate Bill, https://www.gov.il/BlobFolder/news/cyberlawpublic/he/internet.pdf.

39 See Amitay Ziv, "In Lieu of Cyber Defense: The ISA's 200 Million 'Marionette,'" *TheMarker*, August 28, 2018, https://www.themarker.com/technation/.premium-1.6429216; *see also* Part II.A.2.

26 25 24 23 22 21 20 7 6 5 4 3 2 1

The preferred citation for this publication is Elena Chachko, *Persistent Aggrandizement? Israel's Cyber Defense Architecture*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2002 (August 26, 2020), available at https://www.lawfareblog.com/persistent-aggrandizement-israels-cyber-defense-architecture.

About the Author

ELENA CHACHKO

Elena Chachko is a doctoral candidate at Harvard Law School, where she taught comparative foreign relations law. Chachko was previously a postdoctoral fellow at Perry World House, University of Pennsylvania, and a fellow at the Belfer Center, Harvard Kennedy School. She also clerked for the chief justice of the Israeli Supreme Court and worked in Israel's foreign ministry and military intelligence.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION