Some Things the Giant Could Learn from the Small: Unlearned Cyber Lessons for the US from Israel

Eviatar Matania
Lior Yoffe

INTRODUCTION

Over the last decade, cyber threats have grown in magnitude and diversity, and governments devote massive efforts towards adjusting their cyber stance to the evolving threats of the next decade, developing multiple national cyber strategies and dedicated governmental entities to address cyber threats. The responses build on their own and sometimes other countries' experience. For many small nations, however, modest budgets and resources disadvantage their responses. In contrast, Israel succeeded in becoming a cyber success by deliberately leveraging the advantages of being small – Making quick decisions, having the dexterity to change course rapidly, and centralizing national efforts with relative ease. Israel has focused on organizational processes and thoughtful cyber strategy, offering some lessons that could be useful for other nations that are much larger in scale.

This work focuses on where a small country's approach to national cyber security may be relevant for great powers. We examine this issue through the specific case of Israel's advanced, successful cyber approach, which had been quickly developed and implemented through the last decade, and assess its potential adequacy as lessons specifically for the US. The US is a great power, with an area 500 times that of Israel and a population and economy 50 times that of Israel. Our analysis focuses on which of the major elements that Israel focused on may be independent of scale and could also be adopted by a great power such as the US.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Professor **Eviatar Matania** is a tenured professor at the School of Political Science, Government and International Affairs at Tel-Aviv University, where he heads the MA programs in Security Studies and Cyber Politics and Government, and an Adjunct Professor at Oxford's Blavatnik School of Government, where he convenes the Cyber Module. Professor Matania was the founding head (2012-2017) and former Director General of Israel National Cyber Directorate (INCD) in the Israeli PM office for six years, where he reported directly to the PM and was responsible for Israel's overall cyber policy, capacity building, cyber security strategy, and its implementation to defend the Israeli civilian sector. Professor Matania holds a B.Sc. in Physics and Mathematics (Hebrew University of Jerusalem), an M.Sc. in Mathematics with expertise in Game Theory (Tel Aviv University), and a Ph.D. in Judgment and Decision Making (Hebrew University of Jerusalem).

THE ISRAELI CASE

Over the last decade, Israel has become a cyber-defense power by building its cyber capabilities in all dimensions—a comprehensive cybersecurity strategy, new national and governmental organizations, cyber security operational capabilities, and a cybersecurity leading industry (second only to the US), far beyond its relative global size. In this process, Israel developed a comprehensive approach and implemented it through several governmental resolutions, with a strong correspondence between the vision, the strategy, and the structures.

Aiming for a vibrant and sustainable cyber defense ecosystem, Israel's cyber leaders pursued six objectives:

1) national concept of operations

2) operational national cyber agency

3) cross-sector aid to national cyber robustness

4) collocated and collaborating cyber eco-system across industry, academia, and human capital

5) elite cyber teams for techno-operational problems

6) reorienting on countering attackers, not just attacks

These six aspects effectively combined theoretical and practical approaches to cyber security.

First (Policy): A National Concept of Operation to Deal with Cyber-attacks and Attackers as part of an overall National Cyber Strategy

The basic Concept of Operation (ConOp) was designed to be technology and adversary indifferent (to be sustainable through the years), to be cyber native, and to clearly highlight the government versus the private sector roles. The ConOp is comprised of three layers (Matania et al., 2016; Adamsky, 2017). The first layer deals with fostering Market Robustness against daily threats, reducing the nation's surface attack and overall risks. From a governmental perspective, it is executed

Lior Yoffe is one of the founders of the Israel National Cyber Directorate (INCD), currently serving as its Chief Strategy Officer. Prior to that, Mr. Yoffe held several top executive positions within INCD, including the Executive Director for Threat Intelligence, Head of the Cyber Operations Division, and Head of Defense Planning. Thus, he harnesses his vast experience over the years to tackle national challenges in cyber security: Policy, R&D, and operations. Before joining INCD, Mr. Yoffe held various positions in the cyber community in Israel. He also served as Chief Instructor of Talpiot Program, Israel's elite training program for R&D leadership of the Defense Community. Mr. Yoffe holds a B.Sc. in physics and mathematics from The Hebrew University of Jerusalem and an M.A in Security Studies from Tel Aviv University.

mainly by promoting basic cybersecurity hygiene and guiding efforts taken by the private sector through incentives, regulations, and mandatory standards for critical infrastructure, and engaging in awareness and knowledge raising. The second layer is an event-driven tier that aims to tackle cyber threats as they materialize. It defines the national efforts to achieve Systemic Resilience, which focuses on creating situational awareness, tracking threats, handling and mitigating incidents, and promptly sharing information. This involves directly working hand in hand with the private organizations at risk.

While the first two layers concentrate on mitigating attacks, the third layer focuses on the capacity to disrupt cyber-attacks by focusing on the human factor behind them—the attackers—through national defense capabilities. Namely, this layer involves managing a defensive campaign against state-level adversaries, using all national capabilities, traditional and other, such as intelligence, deterrence efforts, law enforcement, etc.

Second (Policy): An operational Central Cyber Agency for National Cyber Defense

Israel's second step was to create a central cyber agency (now part of Israel National Cyber Directorate or INCD), with concrete operational capabilities and the responsibility to defend the national cyber domain and to lead the national cybersecurity efforts.[1] Its role is to implement the three-tier ConOp in operational activities over all the layers. It starts with the Robustness efforts, directly overseeing Israel's critical infrastructure sector as well as working together with other regulators to systematically raise the cyber hygiene of the whole private sector. It continues with leading the national Resilience efforts, mainly through the national CERT and unique analysis and engagement teams where and when needed to mitigate high-risk threats over the civilian sector.

[1] This need was described thoroughly in the paper "Structuring the national cyber defence: in evolution towards a Central Cyber Authority" (Matania et al., 2017)

Finally, INCD leads the defensive campaign and coordinates combined efforts to tackle adversaries with the police, intelligence community, and other relevant security organizations.

Third (Capacity Building): Enhancing National Robustness

A high level of robustness allows the prevention of potential damage from the most common attacks. It raises the threshold of capabilities, and the effort cyber attackers require to penetrate the nation's cyber domain. As the required investment in each attack step rises for attackers, the number of overall attacks decreases.

The INCD chose to address the issue through several vectors. The most well-known is the Israeli approach towards regulating critical infrastructures (CIs). CIs are directly regulated by INCD in a unique way. Each CI has a certified officer within INCD that is trained and authorized to give professional instructions regarding cyber security. In addition, INCD uses the entire spectrum of the regulatory toolbox when facing the entire private market, such as command and controls, standard setting, the duty of disclosure and disclosure regulation, incentives, nudge solutions, raising awareness in the target audience, and more.[2]

Fourth (Capacity Building): Establishing a Cyber Eco-System of Industry, Academia and Human Capital

The INCD took the lead to build a national cyber ecosystem to strengthen its scientific and technological cyber capabilities and innovation processes in the cyber realm to ensure Israel's long-term cybersecurity capabilities.

For this purpose, the Israeli government, through the leadership of the INCD, supported the establishment of research centers in the universities and their work with leading cyber industries; financed high-risk industrial innovation; invested budgets and efforts in enhancing the nation’s human capital in the cyber field; and fostering an ecosystem for mutual enrichment. The most notable example is the unique CyberSpark project in Be'er Sheva, a concentrated and unique cybersecurity ecosystem consisting of Israeli startups, global companies, academia, and civilian and military cybersecurity centers, all within walking distance of one another.

Fifth (Operational): Cyber Commando: Assembling Small Elite Teams to Tackle Tough Techno-Operational Problems

A working group must be small enough to be efficient. In his remarkable book, Northcote Parkinson defined the "coefficient of inefficiency," implicating the size at which a committee or other decision-making body becomes completely inefficient. While being semi-humorous, Parkinson had a point. This notion is of great importance when a nation-state wishes to address the most challenging problems of cyber defense. The core team must be proficient, small, and agile enough to conduct continuous hunting efforts on an ever-changing adversary and should have top experts on its side. The key point is to have a working task force with top analysts in their respective cyber security field, which tackles tough problem, such as identifying

[2] For additional information on the broad regulatory toolbox see for instance Baldwin et al. (2012).

and tracking Advanced Persistent Threats (APTs) campaigns, in innovating techno-operational ways. Israel, being a small country, is accustomed to the logic of small, highly skilled teams that all fit in a small room together. Naturally, it adopted that kind of thinking also in the field of tough cyber defense challenges.

Sixth (Operational): Dealing with Attackers, not only Attacks.

A key element of cyber threats is the existence of a human perpetrator with malicious intent. Accordingly, the third layer of the Israeli ConOp described above consists of national defense efforts, namely the capacity to disrupt cyber-attacks by focusing on the human factor behind them through national operational defense capabilities. These efforts consist of two main vectors. The first focuses on criminal entities through national and international law enforcement mechanisms, mainly police forces and justice systems, while the second concentrates on state-level adversaries looking to harm national interests, whether terror organizations or other countries.

Israel, as a significant cyber power and a leading nation in this field, also sometimes sets the bar in its approach to dealing with national security issues: In May 2019, during several days of heated fighting with Hamas, the IDF destroyed the building of Hamas cyber unit headquarters using fighter jets (IDF, 2019). This unprecedented kinetic response to a cyber-attack showed a first glimpse of the overall thinking in Israel about the way to deal with cyber attackers. This approach was further demonstrated in the recent Guardian of the Walls operation, where several cyber targets (storage facilities, hideouts, and few cyber terrorists) were attacked by the Israeli Air Force and destroyed (IDF, 2021), thus contributing to the deterrence equation between Hamas and Israel.

WHICH ARE THE POTENTIAL LESSONS FOR LARGER NATIONS?

The six major steps fall into three groups for analysis as potential lessons. These are public policy decisions (the ConOp framework and the centralized agency for national cyber defense), capacity building steps (enhancing national robustness and supporting the cyber ecosystem), and operational related steps (assembling elite teams and dealing with attackers).

The first group, the public policy decisions (ConOp and Operational Cyber Agency), is already in progress in the US. A decade ago, there were only a few national cyber strategies and dedicated governmental cyber departments. However, in the following years, there has been a lot of progress on that front, during which many states published their respective national cyber strategies. The US was one of the first to do so. Nonetheless, when it came to establishing a dedicated nonmilitary and nationally operational cyber agency, the US made a significant step in 2018 when it created the Cybersecurity and Infrastructure Security Agency (CISA), the successor of the previous National Protection and Programs Directorate (NPPD). The mission of NPPD was reorganized and broadened into a new agency and prioritized its mission as the federal leader for cyber and physical infrastructure security (DHS, 2018). By doing so, the US has taken a major step forward in assembling an operational agency dedicated to national cyber defense. Overall, following the 2018 act, we see no crucial and potential lesson that can be adapted from the Israeli case in this group.

The second group, the capacity-building steps (Ecosystem and Market Robustness), responds well to scale if pursued strategically and coherently. In most national challenges, scale naturally benefits the US in these areas where bigger is usually stronger. In principle, the larger scale enables more agencies to work on specialized standards and forces them with their larger budgets and more operational options to go deeper into and across all cyber security research agendas. Where Israel has an advanced and strong regulatory framework, it is due to its security culture where the private sector agrees to specific governmental steps. A good example is the concept of certified officers trained in cyber, assigned to each of the critical infrastructures, and supervised closely by the INCD. However, the lessons are almost impossible to apply to the US, but not for scale reasons. Instead, the relations between the federal administration and the private sector are much different, more antagonistic or disconnected; the ecosystem has to cope with a much different security culture and notions of political interaction.

Finally, the third group, the operational steps (Elite Teams and Attacker-oriented Response), is a much more relevant area to lessons that might be adopted by the US in viewing Israel as a pilot state. This is because operational aspects in cyber usually demand agility, creative thinking, and quick reflexes, therefore, they are easier to achieve in small environments and bodies.

The example of small elite teams created by Israel to tackle national challenges in exceptionally difficult techno-operational questions offers particularly useful lessons for US national cybersecurity success. Israel is not the only example. One can see that creating such elite hunting teams also happens within the global cyber industry. Major cybersecurity firms dealing with threat hunting assembled their respective elite teams—Kaspersky Labs' Global Research & Analysis Team (GReAT), Microsoft Threat Intelligence Center (MSTIC), Google's Threat Analysis Group (TAG), and others. Another example of a task force is Google's Project Zero—the team of top security analysts tasked with finding zero-day vulnerabilities. All these teams had tremendous achievements in their super hard missions despite their relatively small number of analysts, and their continuous publications over the years suggest that it was not a one-time success.

The US should consider creating such elite teams beyond those already in the U.S. Cyber Command (USCYBERCOM) or National Security Agency (NSA) to answer the toughest techno-operational questions found in hunting and tracking APT adversaries. These elite teams should be kept small to maintain their quality and agility. Above all, the lesson from Israel is to provide this commando team with a "shielding bubble" focused on their missions to tackle tough challenges, undisturbed by non-essential organizational politics and managerial interference.

Similarly, there are lessons to be learned from Israel's experience to disrupt and deter cyber attackers. The strikes against Hamas cyber attackers during intense operations provided the first glimpse of a new cyber strategic thinking in dealing with cyber attackers in a unique and unprecedented way in the history of the digital era.

Countering the attackers rather than just the attack is crucial for the overall approach towards cyber threats. Israel has shown a glimpse of its overall efforts and thinking on dealing with attackers through the kinetic response against Hamas in 2019 and 2021, which brought together operational, technological, and legal efforts in a timely manner to tackle attackers and enhance deterrence. This lesson needs to be more explicitly learned by the US. Publicly, the US is currently responding to cyber attackers mainly by using indictments and sanctions. We suggest that, as a world leader, the US should carefully consider a more advanced and comprehensive approach to act against cyber adversaries.

SUMMARY

The following table concludes the major step taken by Israel in its approach to the cyber threat during the last decade and their potential adequacy to the US:

Table 1: Israel approach to the cyber threat during the last decade and their potential adequacy to the US.

#	Category	Step	Is there a lesson to learn?
1	Public Policy	Strategy and ConOp formulation	No. US already has vast strategic thinking
2	Public Policy	Centralized agency for cyber defense	No. Already happening with the establishment of CISA in 2018
3	Capacity Building	Enhance national robustness	No. Scale and security culture differences prevent mutual lessons
4	Capacity Building	Support the cyber eco system	No. Scale and security culture differences prevent mutual lessons
5	Operational	Assembling small elite teams to tackle hard techno-operational issues	Yes.
6	Operational	Dealing with attackers	Yes

Israel owes much of its success in the cyber realm to its ability to flip the disadvantages of having a comparatively small budget and few resources into cyber strategy and process advantages that offer lessons in public policy decisions, capacity building processes, and operational capabilities to other states. As such, combined with its unique geo-strategic position, Israel developed several unique approaches towards cyber security, which offer several lessons for the much larger US.

Much of what Israel has done around cyber strategies and new operational organizations to tackle the cyber threat to the nation, as well as its capacity-building mechanisms are either already handled by the US or require underlying conditions not found in the US, such as universal military conscription. These lessons are either unnecessary or not possible for the US to adopt. However, we find that the US could learn several lessons from the Israeli case by carefully examining its operational decisions and approaches. Those steps are relevant not only for small countries but also for larger, especially for the US. Specifically, the as-yet-unlearned lessons are foster small elite (non-military) groups of national cyber specialists ("cyber commando") to put the US in a leading position to tackle high-end techno-operational cyber-attacks, and publicly embrace a more comprehensive and deterring approach to address cyber attackers.

REFERENCES

Adamsky, D. (2017). The Israeli Odyssey toward Its National Cyber Security Strategy. The Washington Quarterly, 40(2), 113-127.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: theory, strategy, and practice. Oxford University Press on Demand.

DHS, (2018, Nov. 13), "Congress Passes Legislation Standing Up Cybersecurity Agency in DHS". Retrieved from: https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs.

IDF. (2019, May 5). “CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed”. Retrieved from: https://twitter.com/IDF/status/1125066395010699264.

IDF (2021, May 21), "Operation Guardian of the Walls", Retrieved from: https://www.idf.il/en/minisites/operation-guardian-of-the-walls/second-week-summary/.

Matania E., Yoffe L., Goldstein T. (2017), “Structuring the National Cyber Defense: In evolution towards a Central Cyber Authority”, Journal of Cyber Policy, Volume II, Issue 1, Chatham House.

Matania, E., Yoffe, L., & Mashkautsan, M. (2016). A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy. Georgetown Journal of International Affairs, 17(3), 77-84.