# Behind Israel's emphasis on Security

*BY DAVID MASSART*
*TUFTS UNIVERSITY*

**ABSTRACT**

Since the birth of the internet, the field of cybersecurity has grown and evolved into one of the largest topics that countries debate in 2019. The field has grown to the point where the DNC deems it an important topic at the Democratic Debates and countries such as China, Russia, and Singapore have started spending more of their federal budget on cybersecurity. Another country who has made notable progress in the cyber realm is Israel, whose 450 active cybersecurity companies spent more than one billion USD in 2018[1]. In 2015, Israeli Prime Minister, Benjamin Netanyahu, promised his nation that they would be "one of the top five cybersecurity powers in the world"[2], and he was right. Israel is now one of the biggest actors in cyber space because of the government's involvement in its technology sector, their military's role as a startup incubator, and generally adopting proactive and efficient cybersecurity policies.

This paper is composed of small segments that provide reasons as to why Israel is one of the largest cyber actors. I will be analyzing Israel's challenging environment, the role of their government and military in their expansion of tech innovation and cybersecurity, the infamous Unit 8200, and Israel's proactive cyber policies. Finally, I will conclude by discussing one of the strongest and important relationships in the cyber realm: US-Israel.

## INTRODUCTION

Throughout the past couple of decades, our society has increasingly relied on digital systems to function and control infrastructure such as airports, industrial systems, and automobiles.[3] This shift in use of technology has inevitably drawn attention to the field of cybersecurity. The emergence of new platforms and new tools leads to the appearance of new vulnerabilities and new ways for attackers to exploit systems. Successful cyber attacks are more frequent and threatening than ever, as adversaries become more persistent[4]. Although there is some hierarchy in the cybersecurity realm, most countries have built their own cybersecurity

---

[1] Halon, Eytan. “Israeli Cyber Investments Exceed $1 Billion for First Time in 2018.” *The Jerusalem Post*
[2] Vice News. "How Israel Rules The World Of Cyber Security | VICE on HBO."
[3] Christopher Kuner et al. The rise of cybersecurity and its impact on data protection
[4] Ibid.

force, tasked to defend the nation against cyber attacks. Around the top of this hierarchy is the United States, one of the most relevant and influential States in terms of research and defense.

Also at the top of cybersecurity is Israel, who helped the U.S develop Stuxnet, a software program that exploded centrifuges critical to Iran's nuclear weapons program in 2010[5]. Nowadays, Israel is one of the most relevant States when it comes to the advancements and research it has accomplished in the field of cybersecurity. It is only in the past two decades that Israel has become "one of the top five cybersecurity powers in the world"[6] and has done so at an incredible, perhaps alarming, rate.

It is interesting to study the possible reasons behind Israel's cyber growth and the methods they use to have such a large impact on other nations and their policies. Israel has burgeoned into a high tech epicenter[7] crafted by its cyber defense technologies. The challenging environment Israel faces in the Middle East, its government's involvement in the technology sector, their military's role as a startup incubator, and the adoption of proactive and efficient cybersecurity policies allowed Israel to grow into one of the most important actors in the cyber space.

## TO THE COMMUNITY

As our society revolves more and more around cybersecurity, it is crucial to know and understand the actors that have the most impact on the field. In particular, Israel is an important actor to look at because of its abnormally rapid growth that has allowed it to affect cybersecurity policy worldwide. Furthermore, it could be beneficial to learn from Israel's tactics and practices when considering our own. Thus, my intent for this paper is to educate on the relevance of Israel in cybersecurity and to spark questions such as: Should Israel be viewed as a threat to US national security? Should the US continue to collaborate with Israel on matters of cybersecurity? What should we learn from Israel when looking at our own security practices? I will not directly be answering these questions in my paper but I simply seek to introduce them and ask that you keep them in mind when reading.

## ISRAEL'S CHALLENGING ENVIRONMENT

Much of Israel's growth in cybersecurity can be attributed to the "challenging environment [it] faces in the Middle East" explains Dudu Mimran, CTO of the Cyber Security Research Center at Ben-Gurion University, located in Be'er Sheva, Israel[8]. September 2000 sparked the start of the Palestinian-Israeli Cyberwar when Israeli teenagers launched a DoS attack that disrupted connections to six websites of the Hezbollah and Hamas organizations in

---

[5] Ibid.

[6] Vice News. "How Israel Rules The World Of Cyber Security | VICE on HBO."

[7] Suciu, Peter. “Why Israel Dominates in Cyber Security.” *Fortune*

[8] Ibid.

Lebanon and of the Palestinian National Authority[9]. Although this so-called "Cyber Holy War" deescalated quite rapidly, the conflict is significant because it presents one of the various experiences that Israel has acquired and learned from in cybersecurity. Mimran goes on to say that "nothing is a substitute for a real hands-on experience [in security] and we've got lots of it."[10]

## GOVERNMENT INFLUENCE

Israel's government has a significant advisory role when it comes to cybersecurity, which allows for the constant collaboration between government, military, businesses, and universities. This is quite unusual because most businesses are reluctant to work with or be seen working with their respective governments[11]. However, part of Israel's success in cybersecurity is due to their proactive government who established both the Israel National Cyber Bureau and the National Cyber Security Authority (NCSA). Since then, the two forces have merged to boost the State of Israel's strength in cyberspace. Israel's Ministry of Foreign Affairs explains from a 2015 press conference that the NCSA "oversee[s] cyber defense actions so as to provide a comprehensive response against cyber-attacks including dealing with threats and events in real time."[12] The government, and especially Prime Minister Benjamin Netanyahu, are committed to investing in cyber because the field is "essential to the security and future of Israel."[13] Furthermore, in 2015, the Cabinet also approved the renewed organization of the cyber defense services sector to better meet cyber threats. These efforts by the government show that Israel is putting an emphasis on cybersecurity and trying to promote collaboration between the private and public sectors in order to maximize their influence in the cyber realm, as well as keep the State secure.

## DIVERSITY WITHIN THE MILITARY AND TECH

Due to the high threat environment described above, Israel has enforced conscription to its military services for all citizens since 1949. The mandatory conscription has allowed the nation to "create a pool of highly trained cybersecurity professionals"[14] by placing them in technical intelligence units. The State can therefore groom its own cybersecurity professionals, which explains why 60 percent of high-tech workers have served in these elite units.[15]

Moreover, by emphasizing diversity in demographics when forming elite units, women make up 35 percent of Israel's tech sector, whereas it is only 25 percent in the United States. The diversification of demographics leads to the diversification of thought and ideas, which could yet

---

[9] Allen, Patrick D., and Chris C. Demchak. "The Palestinian-Israeli Cyberwar." *Military Review*
[10] Suciu, Peter. "Why Israel Dominates in Cyber Security." *Fortune*
[11] Press, Gil. "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry." *Fortune*
[12] "Cabinet Approves Establishment of National Cyber Authority." *Mfa*
[13] Ibid.
[14] Cohen, Natasha, et al. "Cybersecurity as an Engine for Growth." *Cybersecurity Initiative*
[15] Braw, Elisabeth. "How Israeli Conscription Drives Innovation." Foreign Affairs

be another explanation as to why Israel has such an innovation-driven culture. Unit 8200, one of Israel's elite defense force units, uses unconventional recruiting models that build women leaders and serve as an example for the private sector to address the current security talent shortage.[16] Leadership and problem-solving skills are prioritized over technical knowledge because the latter can be taught during training. This creates a diverse environment where juniors are constantly praised and given the opportunity to discuss critical military matters with top commanders[17]. Unit 8200 has taken all these practices into consideration to foster a more diverse and rewarding environment.

**UNIT 8200**

Yair Cohen, a Unit 8200 alum, explained that "90% of the intelligence material in Israel is coming from 8200."[18] The unit has a great impact on Israel's cybersecurity operations. According to Israel's Military Intelligence Directorate, soldiers in Unit 8200 develop and utilize information gathering tools to analyze, process, and share gathered info to officials[19]. It is one of the reasons why Israel is so powerful in the cyber realm -- Unit 8200 has the luxury of picking the 1% of the 1% in the country[20]. As mentioned above, the recruiting process is a little unique and differs from that of the United States' NSA or other agencies because the latter targets experience rather than potential. Unit 8200 also differs from other Israeli military units because the chain of command is less important: "If soldiers feel decisions by superiors are wrong, they can ignore rank and go as high as the commander of the entire unit."[21] This practice builds leadership and soldiers feel ownership over their work. Not only does Unit 8200 impact and drive Israel's cybersecurity, its alumni also end up impacting the rest of the world when they leave to start their own ventures.

Unit 8200 is one of the main examples as to why Israel's military is considered to be a startup incubator. Another alum from Unit 8200, Avishai Abrahami, comments "Just from my generation, there are more than 100 guys from the unit that I personally knew who built startups and sold them for a lot of money."[22] Although the unit is still clouded in mystery, it is well known that large companies such as Wix or Waze were created by Unit 8200 alumni. Through Unit 8200, Israel is able to impact the entire world with its stellar startups and innovation driven culture.

---

[16] Allen, Patrick D., and Chris C. Demchak. “The Palestinian-Israeli Cyberwar.” *Military Review*
[17] Ibid.
[18] Behar, Richard. “Inside Israel's Secret Startup Machine.” *Forbes*
[19] *Idf.il*, www.idf.il/en/minisites/military-intelligence-directorate/.
[20] Behar, Richard. “Inside Israel's Secret Startup Machine.” *Forbes*
[21] Ibid.
[22] Ibid.

## PROACTIVE CYBER POLICIES

For most countries, cybersecurity has been about being reactive to threats rather than being proactive and preventing them. While this is not an ideal approach, it is difficult for many countries to invest in cybersecurity and be proactive about threats that might never arise. However, this is where Israel excels. In the early 2000s, Israel developed their Critical Infrastructure Protection (CIP) policy, that outlines the responsibilities for protecting computerized systems[23]. This policy and the continuous challenging environment that Israel faces ameliorated the cooperation between the defense and the civilian sectors. This has enabled the defense sector to act in a more flexible manner, allowing for innovative thinking. Moreover, the policy shows proactive initiative in the governmental structures[24]. They developed the CIP even before a cyber attack occurred. Proposing proactive policies in cybersecurity is rare nowadays but Israel's motivation to become one of the most influential cyber actors has pushed them to initiate and develop more proactive policies.

## RELATIONSHIP WITH THE US

Israel has close ties to the United States regarding cybersecurity. President Trump's visit to Tel Aviv in May 2017 demonstrates the commitment and the strong relationship between the two countries regarding cybersecurity. Nowadays, America's security partnership with Israel is stronger than ever.[25] There are several reasons why this partnership is crucial for cybersecurity and its future.

First, the two governments launched a U.S.-Israel Cyber Working Group to advance "unprecedented cooperation on cybersecurity through a whole-of-government approach between our two countries on pressing cyber challenges."[26] Government cooperation is crucial in combating threats to national security. The U.S.-Israeli cooperation in the case of Stuxnet is an example of this and demonstrates the large scale effects that cyber intelligence cooperation can have.[27] The damaging cyberattack against Iran's nuclear program is proof that collaboration between cyber superpowers is a valuable weapon and highlights the importance of US-Israel-like partnerships.

Second, U.S and Israel cybersecurity policies are often aligned and in agreement. As an example, Israel was the first country to adopt the U.S. National Institute of Standards and

---

[23] Tabansky, Lior. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Chaire De Cyberdéfense Et Cybersécurité*

[24] Ibid.

[25] United States, The White House. "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017."

[26] Kram, Josh, and Vincent Voci. "U.S.-Israel Cybersecurity Collaborative: A Roadmap for Global Private, Public Partnership." *U.S. Chamber Of Commerce: Above the Fold*

[27] Mercer, Rebekah. "The Importance of the U.S.-Israel Cyber Security Relationship." *Texas Israel*

Technology's best practices for managing and minimizing cyber risk in the public sector.[28] The alignment of policy is important to the development of cybersecurity and lays the groundwork for other countries to follow suit.

Lastly, the private sectors of both countries are always collaborating. Several American companies, such as Oracle, Cisco, Microsoft, and Amazon have set up cybersecurity-focused operations in Israel because they view the country as a cybersecurity hub.[29] Similarly, Israeli startups have recently been "drawn to [Boston] for three main factors: the proximity to customers; the local tech talent; and geography."[30] A large portion of the market in cybersecurity is in the U.S. and a Unit 8200 veteran, Lior Div, explains that you need to move somewhere else if you want to build a meaningful company -- Tel Aviv is not enough.[31] The migration of Israeli startups to Boston has played a major role in "the Massachusetts economy in terms of jobs and economic development"[32] according to Alex Goldstein, the founder and CEO of 90 West.

The alliance between the United States and Israel is crucial for both nations and the rest of the cyber realm. Israel receives military and financial backup from the United States and the latter gives the former a strategic position and an ally in the Middle East.[33] This partnership could very well define the future of cybersecurity and could help shape global policies.

## REFLECTING ON ISRAEL'S CYBER STRATEGY

In my opinion, Israel is on the right track by prioritizing cybersecurity. As our society moves in the direction of a tech driven world, we must consider security at every step along the way. The purpose of this paper is to provide an analysis on Israel's cybersecurity strategy and examine some of the reasons why they have become such a dominant superpower in the cyber realm. Those who read this paper should reflect on exactly why this system works so well and how it has allowed Israel to become this high tech epicenter. They should also reflect on the differences between Israel's strategy and other countries' -- could the US's military act as a startup incubator? By asking ourselves these questions, our society as a whole becomes more aware and more prepared to tackle the challenges of the development of cybersecurity.

---

[28] Kram, Josh, and Vincent Voci. “U.S.-Israel Cybersecurity Collaborative: A Roadmap for Global Private, Public Partnership.” *U.S. Chamber Of Commerce: Above the Fold*

[29] Ibid.

[30] Khalid, Asma. “Why Israeli Cybersecurity Firms Are Moving From Tel Aviv To Boston.” Bostonomix

[31] Ibid.

[32] Goldstein, Alex. “Boston-Israel Cyber Ecosystem Snapshot.” Brandeis News & Media

[33] Mercer, Rebekah. “The Importance of the U.S.-Israel Cyber Security Relationship.” *Texas Israel*

## CONCLUSION

In such a short amount of time, Israel has grown to influence countless countries in cybersecurity. The challenging environment Israel faces in the Middle East, its government's involvement in the technology sector, their military's role as a startup incubator, and the adoption of proactive and efficient cybersecurity policies allowed Israel to grow into one of the most important actors in security. Israel's success in such an important field makes me confident that other countries in the Middle East (or around the world) will be inspired and will follow suit by prioritizing cybersecurity.

## WORKS CITED


Halon, Eytan. "Israeli Cyber Investments Exceed $1 Billion for First Time in 2018." *The Jerusalem Post*, 28 Jan. 2019, www.jpost.com/Israel-News/Investment-in-Israeli-cyber-exceeds-1-billion-for-first-time-in-2018-578906.

Vice News. "How Israel Rules The World Of Cyber Security | VICE on HBO." *YouTube,* uploaded by Vice News, 14 March 2018, https://www.youtube.com/watch?v=ca-C3voZwpM.

Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard, The rise of cybersecurity and its impact on data protection, International Data Privacy Law, Volume 7, Issue 2, May 2017, Pages 73–75, https://doi.org/10.1093/idpl/ipx009

Suciu, Peter. "Why Israel Dominates in Cyber Security." *Fortune*, 1 Sept. 2015, fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/.

Allen, Patrick D., and Chris C. Demchak. "The Palestinian-Israeli Cyberwar." *Military Review*, vol. 83, no. 2, Mar. 2003, www.questia.com/library/journal/1P3-348080751/the-palestinian-israeli-cyberwar.

Press, Gil. "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry." *Forbes*, 18 July 2017, www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#6dc14652420a.

"Cabinet Approves Establishment of National Cyber Authority." *Mfa*, 15 Feb. 2015, mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx.

Cohen, Natasha, et al. "Cybersecurity as an Engine for Growth." *Cybersecurity Initiative*, 21 Sept. 2017.

Braw, Elisabeth. “How Israeli Conscription Drives Innovation.” Foreign Affairs, 19 Apr. 2017, www.foreignaffairs.com/articles/israel/2017-04-19/how-israeli-conscription-drives-innovation.

Allen, Patrick D., and Chris C. Demchak. “The Palestinian-Israeli Cyberwar.” *Military Review*, vol. 83, no. 2, Mar. 2003, www.questia.com/library/journal/1P3-348080751/the-palestinian-israeli-cyberwar.

Behar, Richard. “Inside Israel's Secret Startup Machine.” *Forbes*, 11 May 2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#5b13d2fb1a51

*Idf.il*, www.idf.il/en/minisites/military-intelligence-directorate/.

Tabansky, Lior. “Cyberdefense Policy of Israel: Evolving Threats and Responses.” *Chaire De Cyberdéfense Et Cybersécurité*, vol. 3, no. 12, Jan. 2013.

United States, The White House. “Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017.” *The White House*, 26 June. 2017, https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/

Kram, Josh, and Vincent Voci. “U.S.-Israel Cybersecurity Collaborative: A Roadmap for Global Private, Public Partnership.” *U.S. Chamber Of Commerce: Above the Fold*, 28 June 2019. https://www.uschamber.com/series/above-the-fold/us-israel-cybersecurity-collaborative-roadmap-global-private-public

Mercer, Rebekah. “The Importance of the U.S.-Israel Cyber Security Relationship.” *Texas Israel*, 11 Aug. 2017, www.texasisrael.org/single-post/2017/08/11/The-Importance-of-the-US-Israel-Cyber-Security-Relationship.

Khalid, Asma. “Why Israeli Cybersecurity Firms Are Moving From Tel Aviv To Boston.” Bostonomix, 15 Dec. 2017, www.wbur.org/bostonomix/2017/12/18/israeli-cybersecurity-boston.

Goldstein, Alex. “Boston-Israel Cyber Ecosystem Snapshot.” Brandeis News & Media, 10 Apr. 2018, www.brandeis.edu/global/news/2018/cybersecurity-paper.html.