INSTITUTE FOR POLITICS AND SOCIETY

Israeli inspiration for European cybersecurity

POLICY PAPER / OCTOBER 2020

ADAM VOBORNÍK

WWW.POLITIKASPOLECNOST.CZ

OFFICE@POLITICSANDSOCIETY.CZ

Israeli inspiration for European cybersecurity

Policy Paper – Adam Vobornik, October 2020

Israel has been facing tremendous pressure from its opponents since its foundation in 1948. During more than 70 years of existence, Israel has experienced many wars and tensions still exist today. These experiences have brought the nation to prioritise its security. Simultaneously, these experiences have taught the Israelis to cope with challenges in an efficient way, thus the Israeli approach can be very helpful for Europeans.

With the deepening of globalisation and digitalisation many new threats are emerging. NATO recognised cyberspace as a new battlefield in 2016 and added it to the core task of collective defence. On one side, Israel uses the possibilities of cyber but on the other, they are fully aware of the threats, so they are recognising cyberspace as one of the greatest threats that Israel is facing.

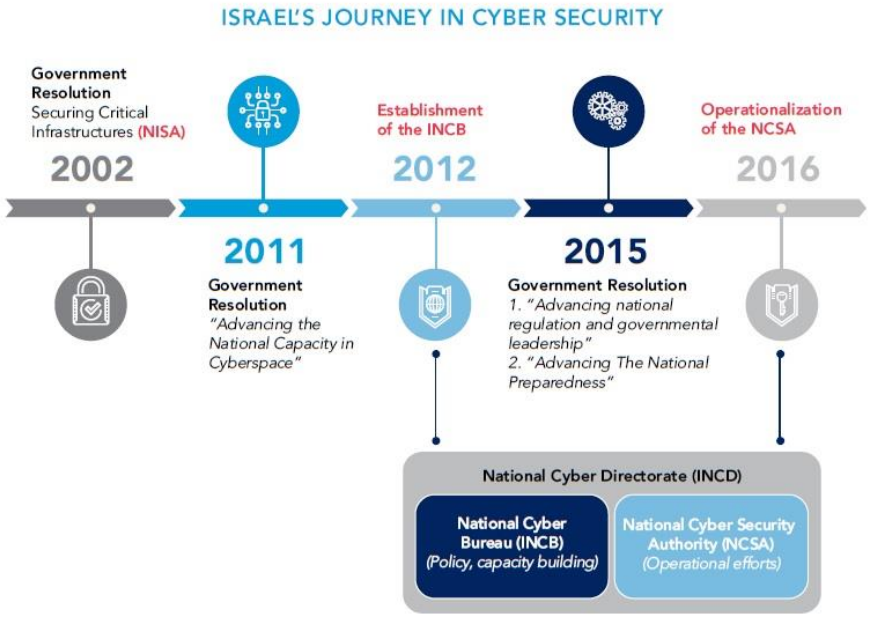
Israeli skills within cyber are extraordinary that is one of the reasons why there are so many companies focused on cyber, from all over the world, with offices in Israel. Moreover, Israel supports the start-up industry which is helping to keep up the advancement and further develop the field.[1]

Israel's successful cyber journey (see scheme below) began in 2002 when National Information Security Authority (NISA) was founded. The agency's aim was to protect and instruct certain systems within private and public organizations. In 2012 the Israel National Cyber Bureau (INCB) was founded, and it is a main breakthrough because it shapes the national strategy, policy and generally improves the capabilities within cyberspace. Later in 2015 the INCB initiated a resolution that later established the National Cyber Security Authority (NCSA), the NCSA directs the operational cyber security efforts. The INCB and the NCSA together make Israel national Cyber Directorate (INCD).[2]

[1] Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. "Israel and Cyberspace: Unique Threat and Response." International Studies Perspectives, 2015. https://doi.org/10.1093/isp/ekv023.

[2] "ISRAEL NATIONAL CYBER SECURITY STRATEGY IN BRIEF," September 2017. http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

Image 1: Israel's journey in cybersecurity



Source: Israel National Cyber Security Strategy in Brief, 2017

What is the philosophy of Israeli cyber security and defence?

Israel has been through very difficult times and their approach towards security is, in general, very exceptional and many countries could learn from it. Israel's geopolitics are harsh, there is no room for mistakes. Some countries and organisations are endeavouring to destroy or damage Israel, therefore security is simply the top priority. The same goes for cyber security and defence. Israel has adopted an approach that is making the country a cyber powerhouse.[3]

Israel's national security concept was built around the so-called *"Security triangle"*. The triangle is composed of *deterrence*, *early warning* and a *decisive operational victory*.

Deterrence is the capacity to intimidate your opponents from attacking you. This is actually happening with Hezbollah. Hezbollah knows that gains would not be higher than costs of the move.

Early warning, because Israel is under constant threat by its Arab neighbours, it is necessary to know what is happening in these countries, as well as having information if there is something that could endanger the state of Israel. The *early warning* system can lead to a pre-emptive attack or in Israel's case, mobilise the reserves in time like during the Yom Kippur War in 1973.

If the *early warning* fails, then there is *the decisive operational victory* which is reliant on the military power that ensures winning the conflict. Another principle was added later: *"army of the people"* which relies on compulsory conscription and mobilisation of reserves. Also,

[3] Press, Gil. "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry." Forbes. Forbes Magazine, July 18, 2017. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#76e9a4494202a.

the Israeli Defence Forces (IDF) were forced to expand in the use of advanced technology, during the Yom Kippur War the IDF was using computerized systems and according to Professor Isaac Ben-Israel this had a direct effect on development and use of advanced weapons and this has lasted until today.[4]

First, the government plays an extremely important role, as it initiated the approach. Benjamin Netanyahu asked Ben-Israel to create a 5 year plan for cyber security on a national level. Eventually, Professor Ben-Israel came up with an ecosystem that is constantly evolving and is ready to face the unknowns. The ecosystem interconnects military, government, private sector and universities. The government has a counselling role. The role of the government is slightly problematic because usually the companies are doing business worldwide, and generally it is not a good sign when a company is working with any government.

The government was vitally important in the beginning phases, and it is equally important in the next phase, as the government works like an impetus, coordinating development. The field of cyber was an exciting opportunity for Israel, because Israel already had a good ground base for research, a practical facility and an advanced high-tech industry. Because Israel needs to maintain its superior position within the MENA region (Middle East and North Africa), the state has found a special way for cooperation between the military, government, and its citizens.

The famous IDF Unit 8200 is a great example. It is producing world-class experts on security. Also, because the soldiers get practical experience, many of its former soldiers are founding start-ups when they finish their military service. This helps to portray Israeli conscription as not a waste of time.

Even though cyber is very often about things that we cannot see or touch, people are one of the most important components. In Israel, they know this and that is why they are investing so much into manpower. The educational system is offering the field of cyber security already during middle school, there are many universities offering cyber security and **Israel was even the first country to introduce a PhD programme focused solely on cyber security**. There is an effective system that helps create and find cyber security specialists.

According to Professor Ben-Israel, technology is truly an indispensable aspect of cyber security, but the field needs to be examined from an interdisciplinary field of view. Meaning that in order to understand cyber security, and all domains are affecting it, it needs to be examined from all disciplines.[5]

Basically, the Israeli philosophy within cyber is a special combination of theory and practice, cooperation within public and private sector, cooperation with government and military, interdisciplinary approach and permanent jeopardy. This combination is making Israel successful within the cyber sphere. The number of global enterprises based in Israel, and Israeli results within cyber, are a proof that the Israeli approach is efficient, and that a lot can be learned from the approach.

---

[4] Baram, Gil. "Israeli Defense in the Age of Cyber War." Middle East Forum. Middle East Forum, 2017. https://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war#_ftn1.

[5] Press, Gil. "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry." Forbes. Forbes Magazine, July 18, 2017. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#76e9a4494420a.

What threats and from which actors are relevant to Israel?

A generally accepted definition of cyberattack is: *"an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization."*[6] Israel like every other state is under the threat of cyber attacks. Cyberattacks are becoming more and more complex and deadly.

It has been proven, by Stuxnet for instance which will be discussed further on, that cyberattacks can do great harm. Beyond that, Israel has many enemies. A lot of nations and non-state actors are considered to be enemies of Israel. With globalisation and cyberspace there are no borders, thus Israel is not only endangered by enemies that are close but also from anywhere in the world.

When it comes to relevant threats emerging from the cyberspace, we can never be sure. The domain is still evolving, it is a never-ending story, that is what makes cyberspace so thrilling. The variety of threats is endless. The national security and economies of almost every state in the world are reliant on technology and intel infrastructure, the internet is at the centre of it all.

The threats can be soft, used during peacetime or also very hard, used during war time. Cyber can even cause loss of revenue or life. Cyber is exploited in espionage. Israel has one of the best intelligence services in the world and this topic is very cloudy. It is believed that espionage is not an act of war, but sometimes it can raise the tensions between states.

Know-how or any other important data can be stolen. It is important to bear in mind how critical intelligence is. Cyber is exploited in propaganda too. Russia is a great example, and they are very good at propaganda. We will never know how exactly the 2016 presidential elections in the USA were affected. Lately, deepfakes are becoming very famous. Deepfakes present to us how cyber propaganda has advanced and how dangerous it is. It will become more and more difficult to recognise what is real and what is fake.

Then, there are economical cyber attacks that can affect economy of a state. The so-called "*Cyber Pearl Harbour*" is frightening for national security. Many people are afraid of such a thing because within cyber there are so many unknowns and unknown unknowns. Generally, cyber can be deadly within any sphere, military or civil. In addition, cyber attacks are not constrained only within the cyber sphere. There are examples when there was a military response to a cyber attack. One of these responses was done by Israelis and it has reshaped the perception of cyber.

As mentioned above, Israel has many enemies, not only states but non-state actors too. On the other side, Israel nowadays has less enemies than in the past. Countries like Jordan or Egypt used to be great enemies to Israel, however that is not true today. Still, there is Lebanon, Syria, Palestine and Israel's biggest rival – Iran. There are many other countries in MENA, Asia and Africa too. From the non-state actors, it is Hezbollah, Palestinian Islamic Jihad, Hamas, ISIS etc.

[6] "Cyber Attacks Explained." IBM, n.d. https://www.ibm.com/services/business-continuity/cyber-attack.

Stuxnet case

The story of Stuxnet describes the threats of cyberspace perfectly. Every cyber security expert is worried that another attack on critical infrastructure will come. The detection of Stuxnet put light on the cyber side of industrial systems and infrastructures. It contributed to caution about strategically important infrastructures and its vulnerability.

The malware was detected in 2010 and surprised experts because the malware was very elaborate. It used four zero-days exploits, meaning that they were not known before. Its aim was to sabotage centrifuges in Iran. It is believed that Israel together with the United States are behind the malware. At that time, it was and today still is in Israel's and US's interest to stop the Iranian nuclear program.

The malware was able to attack networks that are typically isolated from other networks, it was accomplished because the malware was implanted through a USB drive. Iran and its regime looked weak because it was not able to protect its national security priority. Plus, Iran had to spend a lot of money to replace the centrifuge and invest in cyber units. Similarly, like Russia's intervention in Crimea, Stuxnet was a wake-up call for anyone who was not ready. Before Stuxnet, a lot of states were underdeveloped within cyber security, due to this attack, many nations started paying more attention to cyber. Additionally, the tensions in the Middle East were lowered because Iran was slowed down after the attack.[7]

"*On a technical level, Stuxnet uses four different vulnerabilities to gain access to Windows systems and USB flash drives, identified independently by antivirus software makers Symantec and Kaspersky Lab. ... Stuxnet targets individual computers that carry out automated activity in large industrial facilities, but only will activate when it finds the right one. When Stuxnet finds the right configuration of industrial processes run by this software, it supposedly will execute certain files that would disrupt or destroy the system and its equipment. Unlike most sophisticated worms or viruses created by criminal or hacker groups, this worm thus does not involve winning wealth or fame for the creator, but rather aims to disrupt one particular facility, shutting down vital systems that run continuously for a few seconds at a time.*"[8]

Stuxnet would have had much bigger impact if it was not discovered. It had destroyed around 1,000 Iranian centrifuges and slowed down the program. Perhaps the authors of the malware hoped for a bigger impact. Iranians and many other states have realised the new threats and naturally, it is going to be harder to breach the state's cyberspace. However, it raises a question. Has the best chance to disrupt Iranian's nuclear program passed or will there be more opportunities like this one? Certainly, the attack demonstrates that such critical attacks are possible, and increases attention and interest in them. A new complex code base is ready to be examined and modified.[9] It is an example of a cyber threat and the threat can endanger the most crucial infrastructures within any state.

---

[7] Baezner, Marie & Robin, Patrice. (2018). Stuxnet.

[8] Stratfor. "The Stuxnet Computer Worm and the Iranian Nuclear Program." Stratfor. Stratfor, September 24, 2010. https://worldview.stratfor.com/article/stuxnet-computer-worm-and-iranian-nuclear-program.

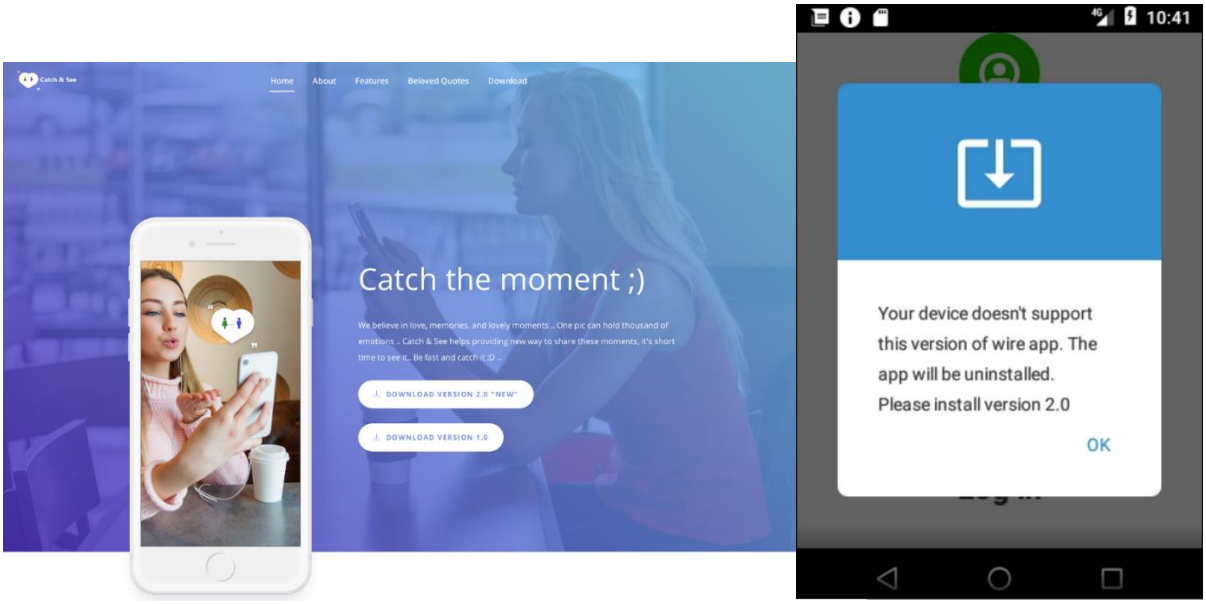
[9] Mueller , Paul, and Babak Yadegari. "The Stuxnet Worm," n.d. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

Hamas's cyber attack

This cyberattack is completely different from Stuxnet. The attack was not focusing on critical infrastructure nor was it as successful as Stuxnet. However, this attack is unique because of its consequences. Israeli intelligence forces were fully aware of the ongoing cyber campaign and intervened controversially. This happened during an escalation in Gaza in summer 2019, when up to 600 rockets were launched towards Israel.

Hamas attacked mobile phones of IDF soldiers using MRAT (Mobile Remote Access Trojan). It was a series of dating apps (GrixyApp, ZatuApp and Catch&See), where Hamas terrorists wrote as seductive women to IDF soldiers and asking to install an application where they can stay in touch. However, when a soldier clicked on the link sent by Hamas, the application was downloaded but it showed an error that the mobile phone does not support the application and the application will uninstall itself. This did not actually happen, and the application only hid the icon. [10]

Image 2: Hamas's cyber attack



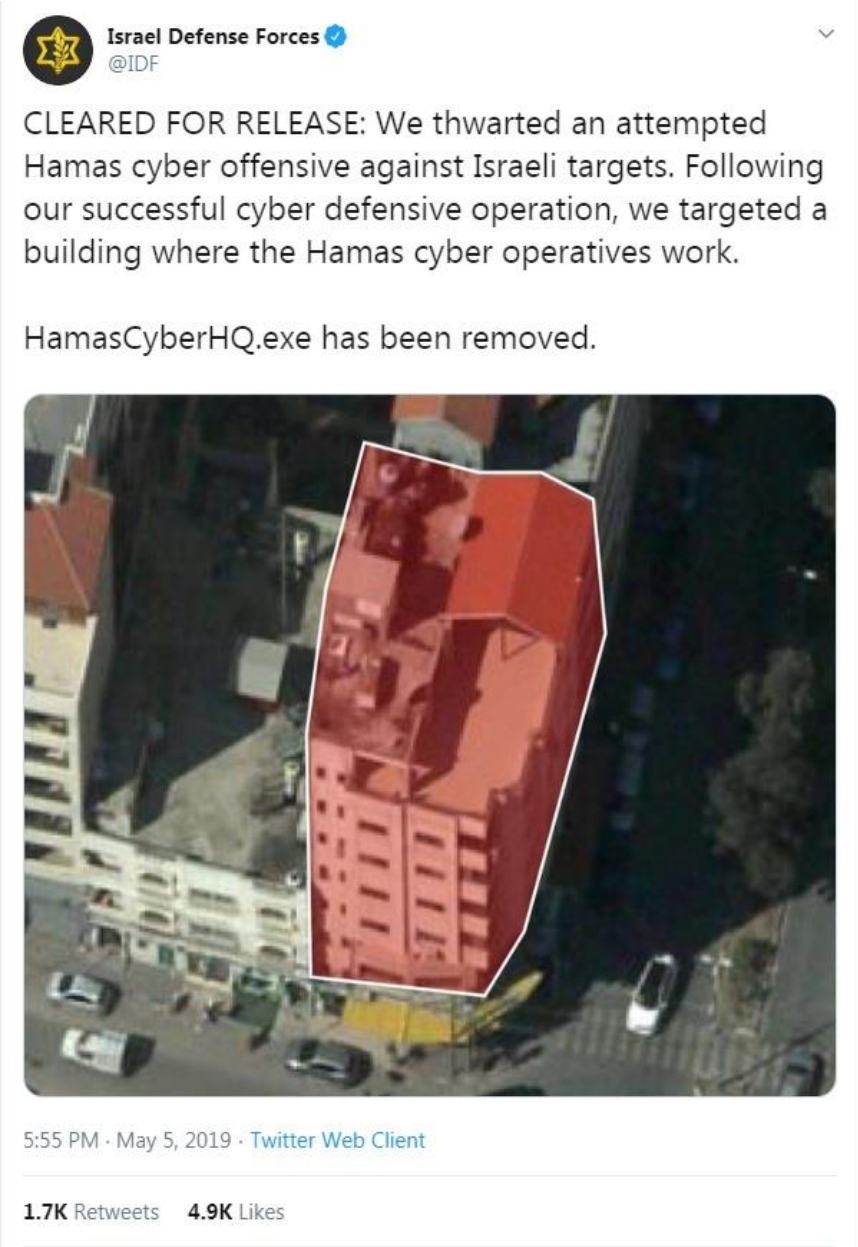
Source: Check Point Research, 2020.

But the application kept communicating through MQTT protocol[11] with the server it was downloaded from. The malware's goal was to gain important data. The app also gained an access to microphone, camera and GPS, so it could endanger sensitive intel when the affected device was nearby something critical. It was created for Android and it appeared very trustworthy as it had its own well designed websites.[12]

In May 2019 there was an escalation going on in the Gaza Strip. Suddenly, the IDF had posted a tweet, reporting that the IDF had targeted a building where Hamas cyber operatives work.

[10] "Hamas Android Malware On IDF Soldiers-This Is How It Happened." Check Point Research, February 18, 2020. https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/.
[11] Protocol that transports messages between devices. More at https://mqtt.org/.
[12] Ibid

Image 3: Tweet of Israel Defense Forces



Source: Twitter of Israel Defense Forces, 2020[13]

This was unique because such an asymmetrical response was taken after a cyberattack. The IDF launched a physical attack as a retaliation for a cyberattack. It immediately raised many questions. Is this the turning point in the evolution of hybrid warfare? Will this become a casual response to a cyberattack?

"Most important in this case is that there was an existing armed conflict ongoing," says Lukasz Olejnik, an independent cybersecurity adviser and research associate at the University of Oxford's Centre for Technology and Global Affairs. "It's an unprecedented event that will be important in the history of cyberconflict. But it is not crossing the line. The fact that

[13] Israel Defense Forces, Twitter Post. May 05, 2019, 5:55 PM. https://twitter.com/idf/status/1125066395010699264?lang=en.

combatants can become targets is not exactly surprising. And as more and more countries treat cyberspace as a domain of warfare, you would have to arrive at this point sooner or later."[14]

Even if Israel was criticised for this response, the campaign recalls that Android system itself is not secure enough and it depends upon contribution by users, developers, manufacturers and elites. IDF stated that Hamas has no cyber capabilities after the airstrike[15], however in February 2020, Hamas struck with a similar but more complex "honey-trap" attack, but the attack was again thwarted by the IDF and intelligence services.

How is cyber perceived institutionally and legislatively?

Generally, Israel is very developed regarding cyber. Fundamental concepts are clear and understanding of these concepts is necessary for further development. That means that terms like *cyber, cyber security* and *cyber defense* are very well understood.

As mentioned earlier, Israel's cyber journey began in 2002 and since then Israel has founded many institutions covering basically all aspects of the cyber arena. For instance, in 2016 the National Cyber Defense Authority was founded. This authority was focusing on a civil sector and its defense of cyberspace. In 2018 the institution was unified under the National Cyber Directorate.[16] Or the CERT (Computer Emergency Response Team), it is another institution, but it is not a guiding or enforcing body but rather it works for the public. Anyone, even individuals, can seek help.[17]

There are many more institutions and it only shows how Israel is developed within cyberspace. Mainly because of historical experiences and the government. The government has set a clear plan and the plan is being followed. It efficiently interconnects institutions with the whole cyber arena. For example, in 2011 the government adopted a plan to become a TOP 5 global cyber power.

If there is a field where is Israel behind, it is definitely the legislation. Israel is struggling to deal with the modern day dilemma of striking a balance between democratic values, technology and human rights. There was not a legal framework for a very long time. However, in the legal drafts from 2018 it could be assumed that the state was looking for more power than it would actually need to have.

It is very difficult to predict the future within cyber and therefore create an appropriate legal framework but it looks like the government is trying to gain more control over its citizens. For instance, the Israel National Cyber Directorate (INCD) would be able to collect security relevant data from the internet and its providers, but the meaning of *security relevant data* is

---

[14] Newman, Lily Hay. "What Israel's Strike on Hamas Hackers Means For Cyberwar." Wired. Conde Nast, May 6, 2019. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

[15] Doffman, Zak. "Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First." Forbes. Forbes Magazine, May 6, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#62f537ceafb5.

[16] Even, Shmuel, David Siman-Tov, and Gabi Siboni. "Structuring Israel's Cyber Defense." inss.org.il, September 21, 2016. https://www.inss.org.il/publication/structuring-israels-cyber-defense/.

[17] Tabansky, Lior, Isaac Ben Israel, Joanna Kulesza, and Grzegorz Małecki. "Building Cybersecurity System in Poland: Israeli Experience," 2017. https://pulaski.pl/wp-content/uploads/2015/02/6d67843d908ede6f344b4392b61b8a83.pdf.

unclear. There are more unclear questions such as: how long can the data be stored, can the data be shared with other agencies etc.

What proves to be the best practice and can be adopted into the European environment?

Even if the European environment is very different from the Israeli environment, there are certain aspects that could be applied in the European environment in order to improve the situation within cyberspace.

The creator of the Israeli success story is definitely its government. It has stated clear goals and has made systems for accomplishing these goals. The systems are interconnecting wide range of actors; military, academia, public, private and all work for the same goal – safe cyberspace and safe Israel. The government also creates good conditions for start-ups, companies and education together with military and intelligence services like actors within the system. The institutions play an important role in the system too. There are several institutions that have a wide range of roles within the system, and thus they are helping to follow the path.

Another aspect is the big investments in the sector. However, this is caused because Israel had already been focusing on high-tech, so there was a certain groundwork already, therefore the investment and research did not need to be so large.

Then, there is the education. The IDF is offering a very good education regarding cyber, and because almost everyone has to go through conscription, the public's knowledge about cyber is very high. Moreover, as mentioned above, Israeli universities are offering programs focused on cyber. Not only universities but secondary schools too. Then, the education meets practical experiences in the army and the result is amazing.[18]

These are the main aspects behind Israeli success story, and they should be adopted within the European environment if Europe wants to maintain its position in the world. Of course, the European environment is completely different than the Israeli, nevertheless, certain moves can be adopted within the European environment.

It is vital to have a system that is improving itself, just like in Israel. But in order to have the system there needs to be major investments into the field of cyber together with crystal clear vision and dedicated work from experts. To maintain the system, Europe generally needs to do better work in introducing and educating cyber to the public. However, this will be much more difficult than in Israel, because not many European countries still do conscription, thus the introducing and educating will require more dedication.

All these practises need to be initiated and guided by governments in the European countries. Because NATO and the EU are realising the importance of cyber, they will certainly push the governments of member states towards more engagement in cyber. The question is, whether the European countries will do enough towards cyber and if they are efficient while reaching the goal. Estonia is another good example like Israel. However, countries in the European Union take the security questions seriously only if they are facing a direct threat.

[18] Ibid

Conclusion

A condition for a successful state in this modern era is keeping up and dealing with the threats and challenges. Israel has understood this logic and is a great example for Europeans on how to deal with this challenging era.

Today, countries are using cyberspace very often. For instance, Russian aggression against Ukraine, the Baltics, and influencing US presidential elections etc. Then, there is Stuxnet or China's espionage campaigns around the world.

What is worrying is that only nations that are either using cyber or have enough resources and are in direct threat are actually taking cyber seriously. Globally, there is a lack of perceiving the importance of, or devoting enough attention towards, cyber security.

Hopefully, the situation will change at least in Europe, because the EU and NATO are finally pushing the member states towards security within cyber. The member states should take countries like Israel or Estonia as an example and use their experiences.

Cyberspace will only be gaining importance, the next sphere that will experience more attention is outer space. In the meantime, the unknowns and unknown unknowns will be coming out and hopefully the European arena will be very well prepared because cyberspace is tremendously important now, and will become even more important in the future.

ADAM VOBORNÍK
Analyst

Adam Voborník completed his bachelor's, in the fields of International Relations and European studies, at the Metropolitan University in Prague. During his bachelor studies, he spent one semester at the University of Lapland in Finland.

Adam finished his master's degree at the University of Haifa in the field of National Security Studies. While he was studying in Israel, Adam was an intern at the Czech Embassy in Tel Aviv where he cooperated with the Czech military attaché.

Bibliography

Baezner, Marie & Robin, Patrice. (2018). Stuxnet.

Baram, Gil. "Israeli Defense in the Age of Cyber War." Middle East Forum. Middle East Forum, 2017. https://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war#_ftn1.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. "Israel and Cyberspace: Unique Threat and Response." International Studies Perspectives, 2015. https://doi.org/10.1093/isp/ekv023.

"Cyber Attacks Explained." IBM, n.d. https://www.ibm.com/services/business-continuity/cyber-attack.

Doffman, Zak. "Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First." Forbes. Forbes Magazine, May 6, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#62f537ceafb5.

Even, Shmuel, David Siman-Tov, and Gabi Siboni. "Structuring Israel's Cyber Defense." inss.org.il, September 21, 2016. https://www.inss.org.il/publication/structuring-israels-cyber-defense/.

"Hamas Android Malware On IDF Soldiers-This Is How It Happened." Check Point Research, February 18, 2020. https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/.

Israel Defense Forces, Twitter Post. May 05, 2019, 5:55 PM. https://twitter.com/idf/status/1125066395010699264?lang=en.

"ISRAEL NATIONAL CYBER SECURITY STRATEGY IN BRIEF," September 2017. http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

Mueller , Paul, and Babak Yadegari. "The Stuxnet Worm," n.d. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf.

Newman, Lily Hay. "What Israel's Strike on Hamas Hackers Means For Cyberwar." Wired. Conde Nast, May 6, 2019. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

Press, Gil. "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry." Forbes. Forbes Magazine, July 18, 2017. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#76e9a449420a.

Stratfor. "The Stuxnet Computer Worm and the Iranian Nuclear Program." Stratfor. Stratfor, September 24, 2010. https://worldview.stratfor.com/article/stuxnet-computer-worm-and-iranian-nuclear-program.

Tabansky, Lior, Isaac Ben Israel, Joanna Kulesza, and Grzegorz Małecki. "Building Cybersecurity System in Poland: Israeli Experience," 2017. https://pulaski.pl/wp-content/uploads/2015/02/6d67843d908ede6f344b4392b61b8a83.pdf.