Building cybersecurity system in Poland:

Israeli experience

Building cybersecurity system in Poland:

Israeli experience

Lior Tabansky, Isaac Ben Israel,
Joanna Kulesza, Grzegorz Małecki

Polskie Sieci
Elektroenergetyczne

Raport powstał dzięki wsparciu spółki Polskie Sieci Elektroenergetyczne S.A.
przy zachowaniu polityki swobody intelektualnej
Fundacji im. Kazimierza Pułaskiego.

Warsaw 2017

Authors: Lior Tabansky, Isaac Ben Israel, Joanna Kulesza, Grzegorz Małecki

Edition: Patrycja Chomicka

Typesetting and composition: Adam Mojski

Building cybersecurity system in Poland:
Israeli experience © Fundacja im. Kazimierza Pułaskiego

ISBN 978-83-61663-11-9

Publisher: Fundacja im. Kazimierza Pułaskiego
ul. Oleandrów 6, 00-629 Warszawa
www.pulaski.pl

Table of contents

Zbigniew Pisarski
Chairman of the Warsaw Security Forum
President of the Casimir Pulaski Foundation

Dear Colleagues,

The awareness about cyber-security has been raised in the recent years. It concerns both the private sector and the policy-makers, causing them to be more involved in developing new strategies that may lead to positive changes concerning their cyber capabilities.

While the development of the non-state actors abilities to defend their data and devices is an important step forward for a more secure society, the most important actors – the states – are usually not that eager to embrace the change. The delay in following the most current trends of defence of the cyber systems – caused collectively by costs, differently structured priorities regarding cyber-security, a lack of proper governmental structures in charge of cyber security – force many of the states to rely on outdated software and defence strategies in the cyberspace.

Although Poland and Israel started building their cyber security systems in approximately the same time (second decade of the 21st century), the difference of approach is clearly visible. Israel is one of the leading states in the development of the cyber security ecosystem – a self-governing structure of both private and public entities that ensure the security of the whole Israeli cyberspace, which is effective in protecting both critical military and civilian infrastructure against possible cyber security breaches. In Poland there is still a strong, on-going competition over cyber security competences without a clear distinction of objectives between many governmental institutions yet there is a room for an improvement of the current system. The issue is even more pressing since there is a strong tendency within the European Union to focus on the changes regarding its cyber security policy presented especially in Tallinn in September 2017.

The Casimir Pulaski Foundation in cooperation with the Blavatnik Interdisciplinary Cyber Research Centre presents the following report that – we hope – will be a further step in the public discussion over the cyber security system in Poland and will allow the Polish decision makers to learn from the Israeli experience.

Zbigniew Pisarski

Chapter 1

Cybersecurity in Israel: why the success?

Lior Tabansky, Isaac Ben Israel

How to succeed in providing national cybersecurity? This question tops policy agendas for many European governments – and rightly so. Israel is acknowledged as a global cybersecurity leader, encompassing strategy, defense, research, capacity building, technology, entrepreneurship and human capital. Comprehensive cybersecurity for the civilian sector has become the focus of Israeli policy, as sectorial cybersecurity matured in defense, government and Critical Infrastructure has been achieved. Having studied and contributed to the development of several national cyber strategies for years, we have developed a unique analysis on which this chapter builds.

Measuring success: Innovation indicators of Israel

In 2011, the strategic goal of making Israel one of the top-five global cyber powers by 2016 was adopted.

At the government assembly held on 15 February 2015, the head of the Israel National Cyber Bureau (INCB) presented the Israeli cyber industry record achievements in 2014:

- 30 early-stage cyber firms raised over 200 million USD in funding: a 40 % increase over 2013;
- Eight Israeli cyber companies were purchased by foreign investors for an overall sum of approximately USD 700 million.

Later indicators are encouraging:

- Current estimates are that 15% of the global private cybersecurity R&D funding go to Israel (2017);
- 60 cybersecurity companies were founded by Israelis in Israel in 2015; 65 in 2016;
- A different survey found 81 newly founded cybersecurity startups in 2015; 83 in 2016;
- Cybersecurity exports by Israeli companies were later estimated at approximately USD 3 billion in 2013, three times greater than the United Kingdom's. The Economist published that the volume of Israeli cybersecurity exports jumped to 6 billion USD in 2014, second only to the U.S., and three times higher than the *target* the UK set for 2016.[1]

These achievements clearly build upon the innovation system, which focuses mostly on developing computing, software and electronics technologies.

The global 2017 Bloomberg Innovation Index[2] ranked Israel:

- 10th overall in 2017;
- 1st in researchers and scientist concentration;
- 2nd in R&D intensity;
- 3rd in High Tech density.

Additional indicators include:

- Three of the seven Israeli universities (Technion, Tel Aviv University and Hebrew University) consistently rank in the world's top 100 best universities;
- Tel Aviv university is ranked 22nd in the number of citations per faculty (QS 2016);
- Tel Aviv University is ranked 9th in the number of VC-backed startups and the 1st outside the U.S. (Pitchbook 2016);
- Israel has more companies listed on NASDAQ than any other country besides the US and China;
- Israel has the highest density of start-ups in the world
- Counting from 3,100 to 4,200 active tech start-ups, Tel Aviv ranks fifth in the world for best start-up cities, the top outside the U.S.[3];
- Israel attracts more Venture Capital per capita than any other country;
- Israeli cybersecurity start-ups raised $581 million in 2016, 9% more than in 2015 – second only to the amount raised by American cybersecurity firms during the year;
- Over 250 multi-nationals have an R&D Center in Israel (most focusing on IT);
- Israel's Defense and intelligence agencies have earned formidable reputation in developing and effectively using cybertechnology for operations of high strategic importance.

We now turn to analyze the Israeli cybersecurity case study, focusing on the strategy development process and the following selected policies to facilitate cooperation

[1] *Israel's Computer-Security Firms: Cyber-Boom or Cyber-Bubble?*, Economist 411, 2015 , No. 8945.

[2] *The Terminal*, Bloomberg Professional Services, accessed on: 26th of October 2017, available at: https://www.bloomberg.com/professional/solution/bloomberg-terminal/?utm_source=bcom-bn&bbgsum=dg-ws-core-bcom-bn.

[3] *The Global Startup Ecosystem Report 2015*, Compass, accessed on: 26th of October 2017, available at: https://ec.europa.eu/futurium/en/system/files/ged/the_global_startup_ecosystem_report_2015_v1.2.pdf.

between sectors and stakeholders towards the desired ends. The analysis demonstrates the crucial role of policy in developing cybersecurity through cooperation for innovation.

Explaining success

The common explanations for Israel's extraordinary performance refer to cultural characteristics and geo-strategic environment, which allegedly created a dire need for successful innovation:

- Cultural characteristics of the Jewish state, including the high value that families place on education and the risk-welcoming mindset that supports entrepreneurship and does not socially penalize failure.
- The tough geo-strategic environment, that resulted in decisions to establish compulsory military service for men and women, and maintain the highest defense expenditure in the developed world.

These reasons are correct but they are only partial explanations.

The government plays the main role, which is often overshadowed by the media's attention to business aspects and the general fascination with technology. The underlying reasons for Israel's success are long-term strategic efforts by the government to spur and support innovation creation and absorption. These deliberate policies have laid the foundations for the national innovation system in general and for cybersecurity in particular.

According to the OECD:

> *While the success of the Israeli system is primarily attributable to vibrant business sector innovation and a strong entrepreneurial culture, the government has also played an instrumental role in financing innovation, especially in SMEs, and in providing well-functioning framework conditions for innovation, including venture capital (VC), incubators, strong science industry links, and quality university education.*[4]

In fact, Israeli governments of opposing parties have made common strategic choices of investing in the national innovation system. The leadership established the ends, surveyed the means and designed a high-level strategy to match the means to the ends, all while securing political feasibility by taking into account the fundamental values and specific requirements of the relevant stakeholders.

National Cybersecurity is also a strategy and policy issue, where political factors play a crucial role. Acquiring and implementing technical capability should be the result, not the replacement, of such a strategic process.

Strategy, policy, governance

Though some elements of the defense and intelligence community have long had leading experience with leveraging cyber technology for their missions, such efforts took definite shape in the Israeli government only in the mid-1990s. Defense leaders filled the knowledge gap in the civilian branches of government which facilitated cybersecurity efforts, culminating in the first centralized Critical Infrastructure Protection (CIP) (2002) policies in the developed world. The government takes the lead role in providing national cybersecurity by providing mandatory professional guidance to private and public organizations that operate Critical Infrastructure. The shared responsibility arrangement, where Israel's *Re'em* (National Information Security Agency (NISA)) within the (Israel Security Agency (ISA)) was a professional regulator, proved viable. However as cyber technologies continued to develop and penetrate the society, so did the risks and threats. In response, the PM tasked Isaac Ben-Israel to lead the 2010 National Cyber Initiative. This external, multi-stakeholder expert review committee pursued a comprehensive approach, that looked beyond reducing threat vectors and explored macro-economic and strategic benefits for Israel. The National Cyber Initiative taskforce considered the existing cybersecurity efforts

[4] *Science and innovation: Country Notes. Israel*, OECD, accessed on: 26th of October 2017, available at: http://www.oecd.org/israel/41559762.pdf.

[5] *The National Cyber Initiative – a Special Report for the Prime Minister*, The Supreme Council on Science and Technology, Jerusalem: Ministry of Science and Technology National Council on Research and Development, 2011.

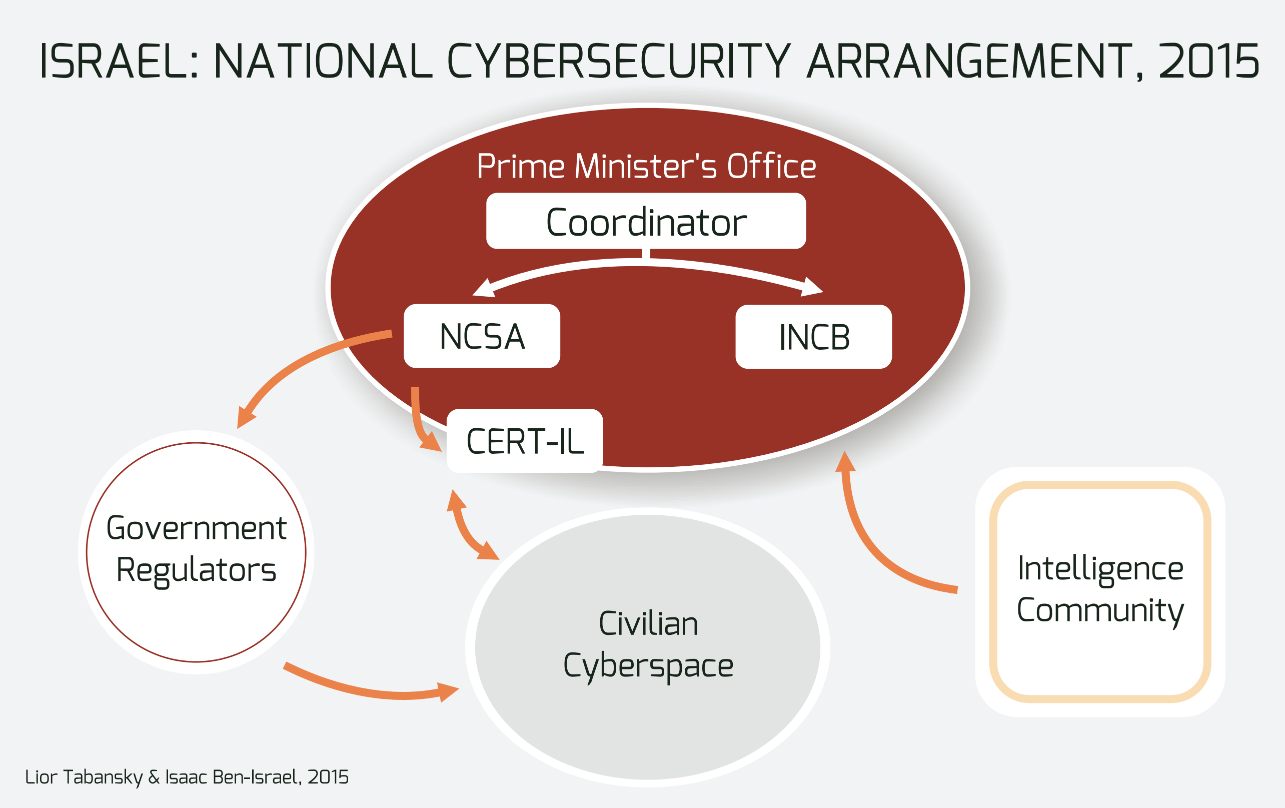
inadequate to the rapidly changing environment. Increased collaboration of government, defense, academia, and industry in the Israeli ecosystem was put forward as the best strategy to enhance national cybersecurity and reach the strategic goal of making Israel one of the top-five global cyber powers by 2016.[5]

The 80 government, defense, academia, and industry experts working in 8 subcommittees for 6 years presented over a dozen recommendations. The shared theme was the need to promote innovation by boosting capabilities and collaboration in the Israeli ecosystem.

The Government Resolution No. 3611 of August 7, 2011 'Advancing National Cyberspace Capabilities'[6] accepted the National Cyber Initiative's recommendations, becoming Israel's public National Cybersecurity Strategy. Cybersecurity strategy of Israel puts forward two interrelated goals: on one hand mitigating security risks, on the other leveraging opportunities enabled by the developing cyberspace.

To develop and implement the strategy, a new Israeli National Cyber Bureau (INCB) was established in the Prime Minister's Office, tasked with policy design and coordination functions. Among the INCB's central tasks was promoting research and development, while boosting the export-oriented cyber industry in Israel. Dr. Eviatar Matania was named head of the INCB, and remains in duty in Autumn 2017. Since 2012, the INCB had indeed been able to drive significant academic research efforts, an export-oriented cyber-industry, professional education, and international cooperation agreements.

The government resolved in February 2015 to establish a new National Cyber Security Authority (NCSA) designed to enhance comprehensive national cybersecurity while reducing the tension between basic freedoms and security. The INCB and the NCSA would form the National Cyber Directorate where they would work independently alongside each other. This process includes multiple legislative,

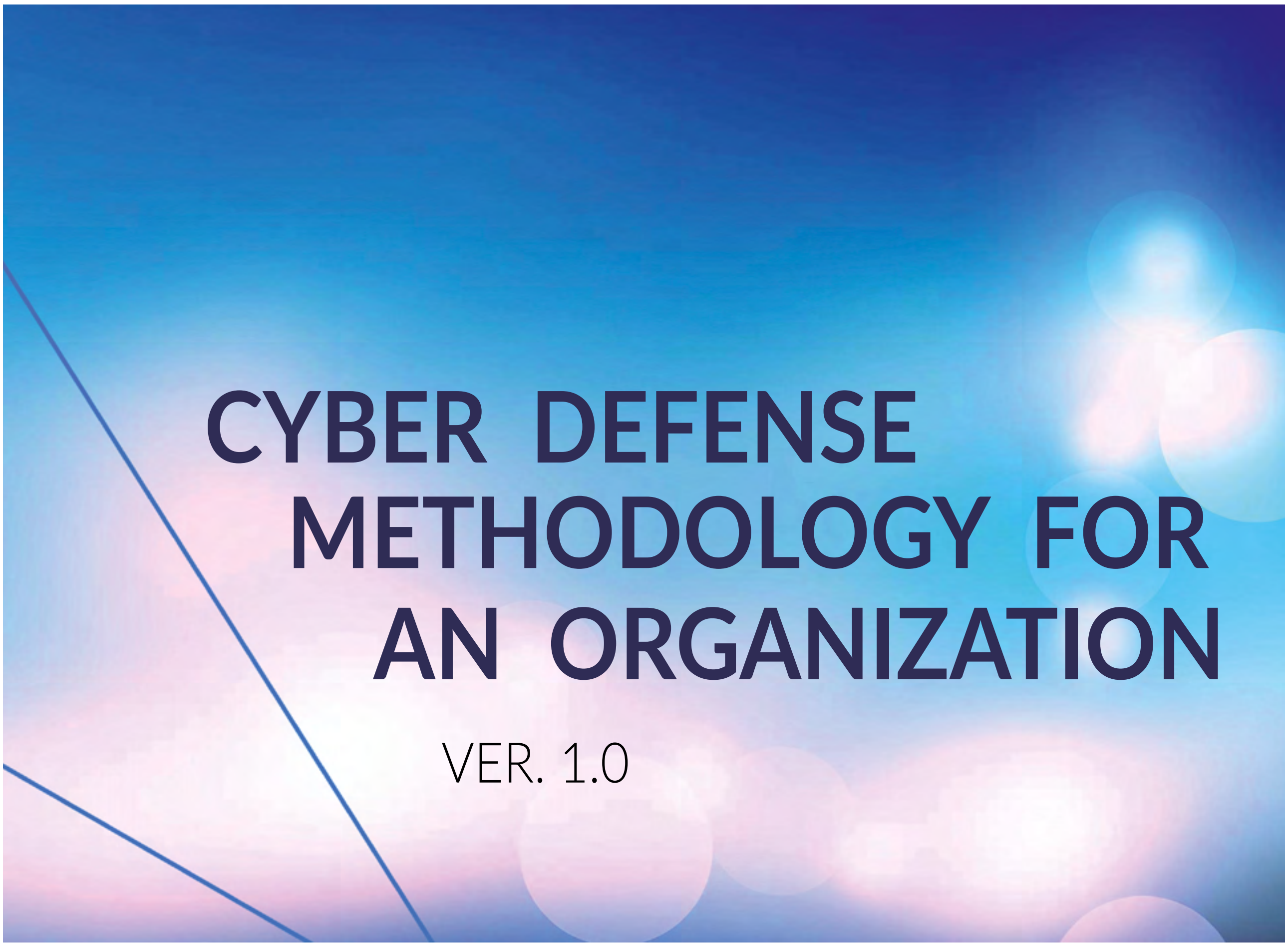


1. Israel: national cybersecurity arrangement, 2015[8].

[6] Government decision 3611: *Promoting national capacity in cyber space.* Jerusalem, Israel, PMO Secretariat.

[7] *National Cyber-Defense Authority*, Prime Minister's Office, accessed on: 26th of October 2017, available at: https://www.gov.il/he/Departments/about/newabout.

[8] Tabansky, L. and Ben Israel, I., *Cybersecurity in Israel*, Springer International Publishing 2015.



CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION

VER. 1.0

organizational, and other efforts estimated to last several years.

The scope of NCSA is enhancing cybersecurity throughout the entire civilian (non-defense) sector, attentive to firms of all levels of economic activity as well as private individuals. Using an Air Force analogy, INCB focuses on force buildup, while NCSA focuses on operations.[7] Overall, the NCSA will refrain from performing any law-enforcement activities, in order to facilitate cooperation with all relevant stakeholders in the society.

Under a temporary order in place until 2018, Baruch Carmeli was named head of the National Cyber Authority. During the annual CyberWeek held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at the Tel Aviv University in June 2017, the NCSA held a one-day first exposure event, introducing its leadership and plans to a 600-strong audience.

The CIP units are being transferred into the NCSA. Catering to non-critical sectors, The National Computer Emergency Response Team (CERT-IL) is located in the Be'er Sheva SPARK complex and has begun operations as a public central contact point for support. The NCSA is developing both the concept and the technology to enhance the national situational awareness in cyberspace through cooperation. CERT-IL is a crucial element, as it must be accessible to any civilian, with developing channels to work with sensitive data and clandestine agencies. The process has already resulted in contracts with an industrial consortium led by the Israeli defense contractor RAFAEL.[9] Further, the NCSA has published a common accessible instruction "Cyber Defense Methodology for an Organization[10]" in June 2017, after extensive consultations.

[9] *First Published: IBM, EMC, Matrix, Cisco and Rafael to establish the National CERT*, IsraelDefense accessed on: 26th of October 2017, available at: http://www.israeldefense.co.il/en/content/first-published-ibm-emc-matrix-cisco-and-rafael-establish-national-cert.

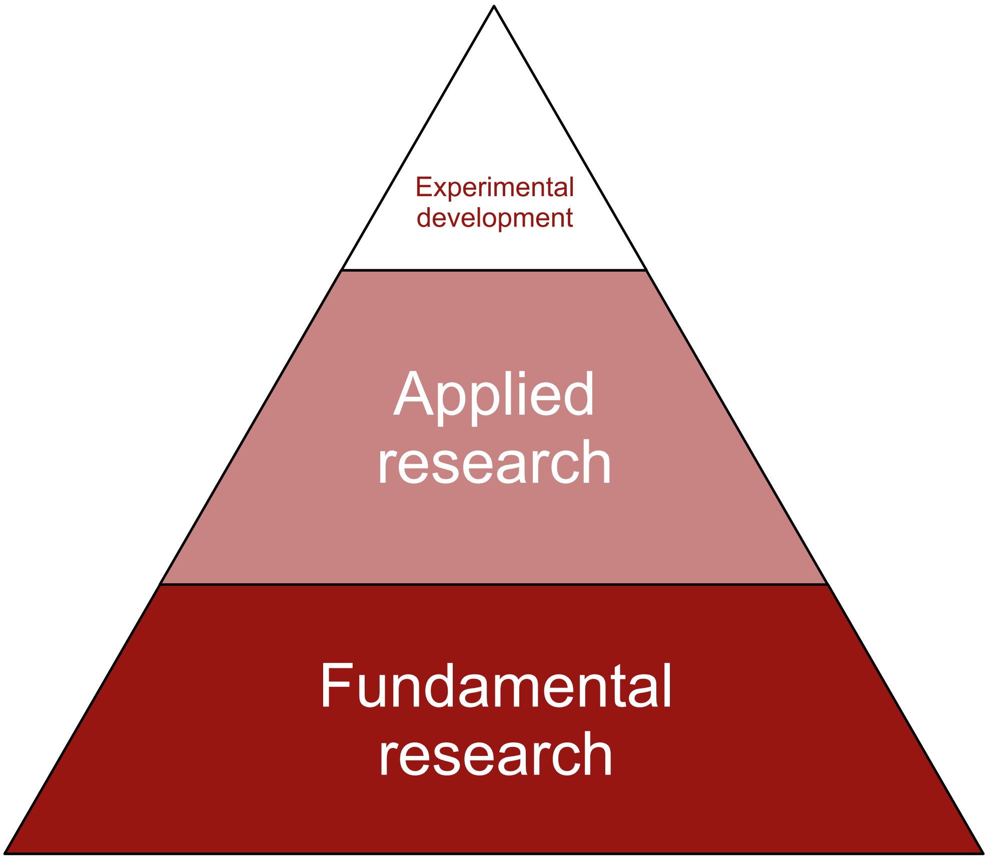
[10] *Cybersecurity Methodology for organizations*, Prime Minister's Office, accessed on: 26th of October 2017, available at: https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

Government & Defense

Having presented the current strategy and policy, it is important to note the long-standing cyber efforts in the civilian government as well as in defense.

In 1997, the *Tehila* (the Government Infrastructure for the Internet Era) unit was established in the Accountant General's office in the Ministry of Finance to provide the government branches with primary services towards a unified secure IT infrastructure for the whole government; secure internet access to government services, from the office and later from home; secure hosting of government websites and e-government services and secure infrastructure to support various future government projects. Throughout numerous organizational challenges, the *Tehila* unit was successful in securing government IT infrastructure, developing unique expertise as well as numerous professional cadres. The Government ICT Authority (Information and communications technology) was established in 2012 as the Government ICT headquarters in the Ministry of Finance, incorporating the previous units. Since January 2015, the Authority has been transferred to the Prime Minister's Office.[11] Today, the main goals remain effective and secure e-Gov services, designed with the INCB.

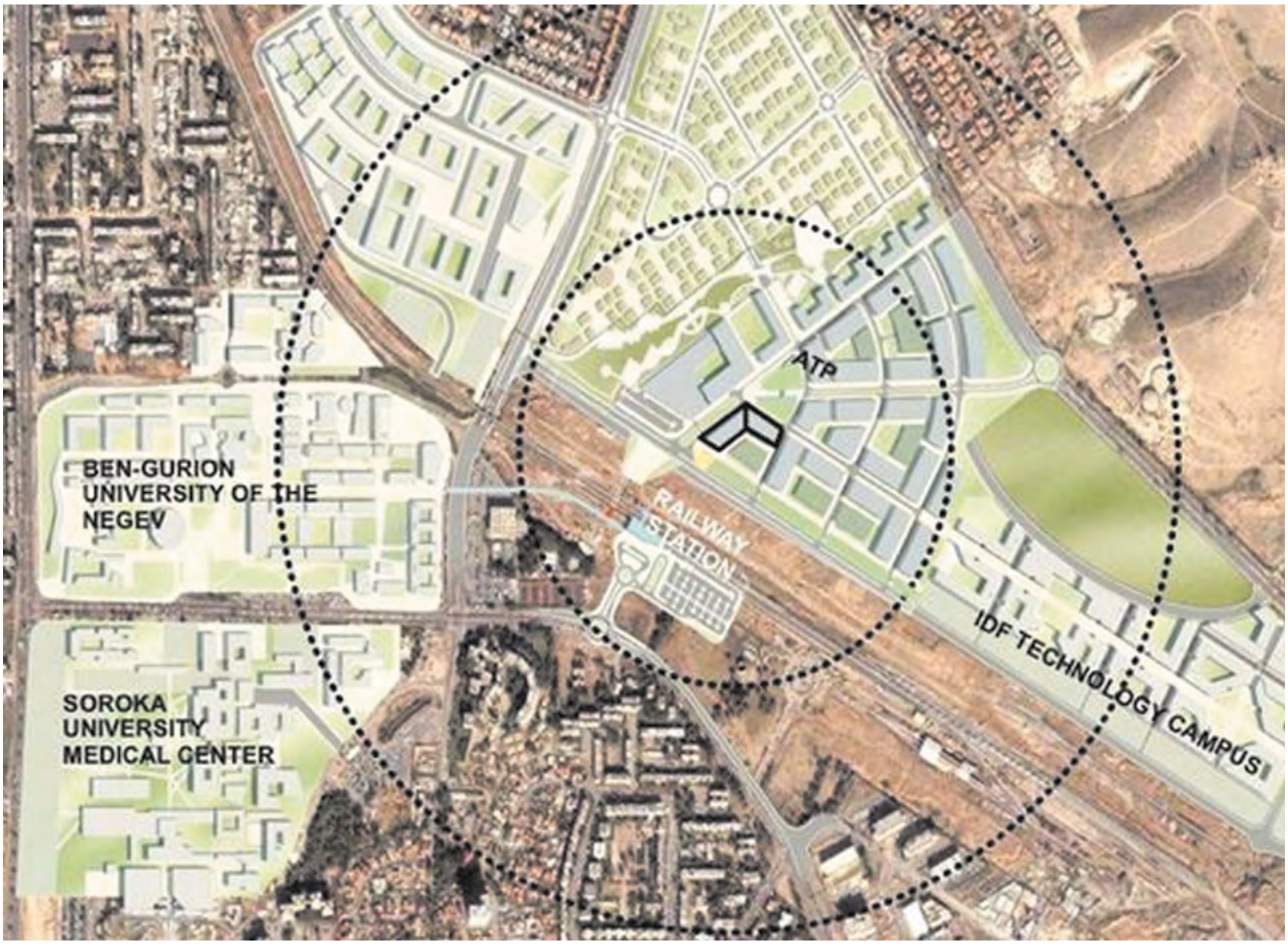
The Israel Defense Forces (IDF) have a long history of advanced electronic and cyber warfare. However, the IDF continues to be baffled with the question of how best to organize the cyber issue. At the beginning of his tenure as IDF Chief of Staff in 2015, Lt. Gen. Gadi Eizenkot announced he would bring together the military's cyber units under one body, a command unit on par with the Ground Forces, the Navy or the Air Forces. In June 2015, the IDF announced their decision to establish a new Cyber Command in two years. Notably, it is unclear what sort of organization it will be. "The IDF cyber *command* will be directly subordinate to the Chief of Staff; this *arm* will be the fifth such *branch* within the General Staff."[12] The authors, INSS experts, conflate three



2. Fundamental and applied research.

[11] *Government ICT Authority*, Prime Minister's Office, accessed on: 26th of October 2017, available at: https://www.gov.il/en/Departments/government_ict_authority.

[12] Siboni, G. and Elran, M., *Establishing an Idf Cyber Command* in *INSS Insight*, Tel Aviv Institute for National Security Studies INSS, 2015.


BEN-GURION UNIVERSITY OF THE NEGEV
SOROKA UNIVERSITY MEDICAL CENTER
ATP
RAILWAY STATION
IDF TECHNOLOGY CAMPUS

3. Cybersecurity industry cluster in Be'er Sheva

distinct terms - command, arm, branch - in a single sentence about the decision. In the same paragraph, more information is added: "Among the four existing branches, the air force, navy, and intelligence are responsible for both the buildup and operational deployment of their respective forces, while the ground forces command is responsible solely for the buildup of its force, with the operational deployment carried out by the territorial commands. The cyber command will apparently be charged with both the buildup and the operational missions of the force." The decision to establish a new Cyber Command was a response to the longstanding need to integrate the IDF's cyber defense and offense. This has been, and will likely remain a challenging process as the General Staff's C4I branch currently bears primary responsibility for defending all IDF communications and computer-based systems, whereas the Intelligence branch is responsible for cyber exploitation and offense. However, in May 2017 it was published that the IDF reversed the decision: the Military Intelligence will lead collection and offensive operations, and C4I corps will lead defense of IDF assets.[13]

University & Education

Fundamental research depends on government expenditure, often due to defense needs, and the research institutions that perform basic research are typically universities. Academia drives and performs most of basic science and fundamental R&D. This is a constant phenomenon worldwide: the business sector is unwilling and unable to undertake fundamental research. Almost all business R&D is applied research: using mature basic science to develop applications for business needs, with a typical time horizon of a few months up to several years at best.

Despite the large share of the business sector in cyber R&D in Israel, a historical analysis will demonstrate that business R&D relies upon

[13] *IDF Scraps Plans for a Unified Cyber Command*, IsraelDefense, accessed on: 26th of October 2017, available at: http://www.israeldefense.co.il/en/node/29613.

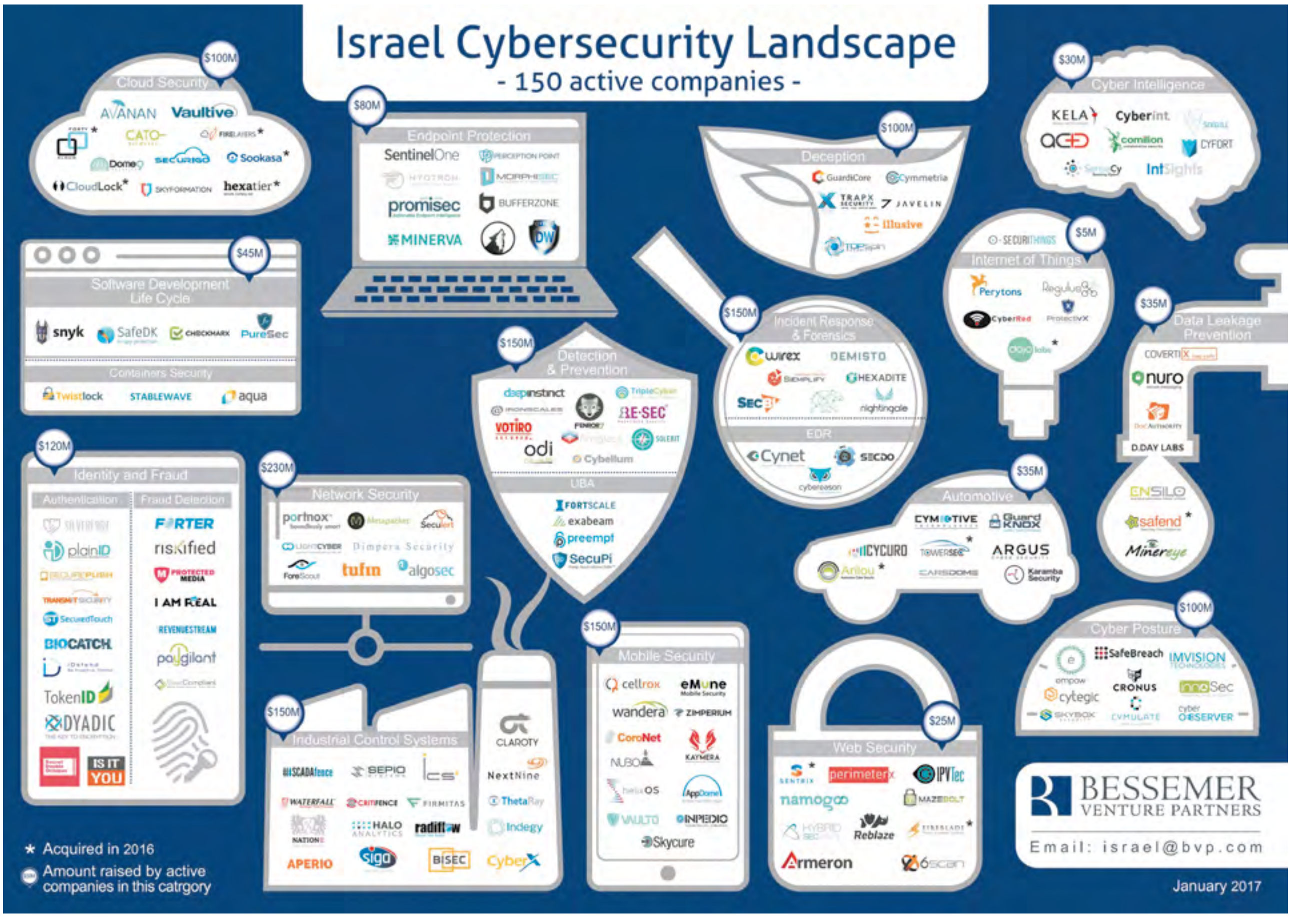
consistent government support for fundamental research.[14]

As of Q1 2017, five of seven Israel's research universities established Cyber Research Centres supported by the INCB. The INCB developed a model where it funds part of the research budget, on the condition that the university matches it with additional funds from new sources. Still, the government refrains from commanding innovation processes: the grant allocation is guided by the standard academic criteria of research excellence. Inaugurated in September 2014, Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Centre (TAU ICRC) is the first institutionalized Israeli government-academia partnership. TAU ICRC is by far the largest one, having already supported over 60 research projects and bringing together around 50 faculty members and over 200 researchers.[15] In addition to science and engineering, TAU ICRC also conducts policy research, as well as public outreach such as the CyberWeek annual conference.[16]

Industry & Business

The INCB contributes to the establishment of an additional cybersecurity industry cluster in Be'er Sheva, collocating the government CERT, military intelligence and the technology units, the Ben Gurion University, multinationals and local businesses.

The Advanced Technology Park (ATP), also known as CyberSpark[17], is at the core of the ambitious implementation of the current expertise in innovation ecosystem development in a given geographical region. The goal is not only to replicate the successful Tel Aviv area, but also steer innovation towards



4. 150 active cybersecurity companies in Israel - BVP 2017

[14] *Trends in Israel's GERD GDP ratio, 2006–2013*, Getz et al., 2013, accessed on: 26th of October 2017, available at: https://commons.wikimedia.org/wiki/File:Trends_in_Israel%E2%80%99s_GERD_GDP_ratio,_2006%E2%80%932013.svg

[15] *Report 2014-2016*, Blavatnik Interdisciplinary Cyber Research Center, accessed on: 26th of October 2017, available at: https://icrc.tau.ac.il/Report

[16] *Cyber Week*, accessed on: 26th of October 2017, available at: https://cyberweek.tau.ac.il/

[17] *Israeli Cyber Innovation Arena*, accessed on: 26th of October 2017, available at: http://cyberspark.org.il

cybersecurity specialization. The government provides infrastructure and incentives, such as the refund of up to 20% of every cyber-related employee's gross salary to commercial cybersecurity entities that set up their business in ATP.

There are at least 150 active cybersecurity companies in Israel, the vast majority are in fact start-ups and young firms[18]. The future of cybersecurity innovation will be the fusion between traditional realms and new possibilities, not in doing same things more efficiently. Today it becomes clear that Enterprise IT is just one part of cybersecurity. Operational Technology controls all vital societal processes – and it depends on cybersecurity. On top of the vibrant innovations in the Industrial Control Systems (ICS) security, Israel is becoming an unlikely automotive powerhouse. Since 2015, seven new companies were founded to develope solutions for the next big leap in automotive technology- safe and secure self-driving cars. More recently the IOT landscape emerged; some ten new companies were founded were founded in Israel that focus on the yet-to-mature IOT challenges.

Innovation capacity is the solution

This chapter has presented the Israeli case study where it illuminated the development of innovation through several diverse cooperation mechanisms between stakeholders from different sectors, all interconnected through a coherent strategy and supported by government agencies.

It is tempting, both for the decision maker and the adviser, to prescribe a definite strategies and courses of action. In cybersecurity, we must argue against such an approach. The sobering lesson of international history is that although it is usually better to have some kind of strategy than not, unless you are prepared to adapt it as circumstances change, it is unlikely to do you much good (Freedman, 2013). Information and Communication Technologies (ICT) evolve at an exponential pace, as predicted and described by Moore's Law in 1965. Fusing the lessons of strategic history with the exponential rate of technological change results in a humbling perspective on cybersecurity strategy. Innovation remains the best chance to adapt in a timely and effective manner to the inevitable change. To spur innovation, cooperation mechanisms between stakeholders from different sectors needs to be designed and facilitated. No other than the government is better positioned to achieve these goals. Moreover, the Israeli success attests to the feasibility of effective government strategy and policies in innovation for cybersecurity.

[18] *Israeli Cybersecurity Landscape*, Bessemer Venture Partners, accessed on: 26th of October 2017, available at: https://www.bvp.com/sites/default/files/files/strategy-resource/Israel%20Cybersecurity%20Landscape%20January%202017.pdf

Chapter 2

Cybersecurity in Poland

Joanna Kulesza

Policy background

Poland has been struggling with the cybersecurity challenge since 2008. While its primary obstacle lies in effective policy making for this particular area of state activity, as will be discussed further herein, the general economic structure of state funding remains relevant. A representative indication of a countries policy priorities can be found in its budget distribution. Poland's entire research funding for 2017 amounts to 8,4B PLNs (est. 2,3B USD) with further 16B (4,4B USD) directed at higher education, distributed among various institutions. No cybersecurity research budget has been directly identified, as Poland lacks a coordinated cybersecurity research strategy, reflecting the decentralized cybersecurity landscape in all other policy aspects.

State policy priorities as reflected in the current (2017) budget focus on social security with a budgetary expenditure of 85,2B PLNs (est. 23,6B USD) and 60B PLNs (17B USD) going to local governments, funding primary and secondary education, again with no particular focus on cybersecurity awareness or IT training for early stage students. Poland's economic plans fail to reflect the guiding principles adopted in e.g. Israel, where the central budget contributes to private investments in cybersecurity in equal parts.

Deficient, not industry-oriented, research policy is one of the reasons why Poland lacks a competitive business position on the global agenda. OECD notes:

> *As foreseen in the government's responsible development plan, stimulating private R&D spending and improving research quality and university-industry collaboration will be essential to improve Poland's ability to innovate and adopt new technologies to move towards higher technology production and strengthen trade prospects. Too many adults have low skills; improving their access to training while strengthening firms' engagement in vocational education would ensure that globalisation benefits are shared more widely.*[19]

According to the CWUR ranking, Poland's top university placed 429th (Jagiellonian University) with the University of Warsaw ranked at 449 and the Warsaw University of Technology at 666[20]. The table below demonstrates the striking discrepancy between research performance in Poland and Israel. While Poland has been struggling with its post-communist legacy of state funded higher education and attempts to incite industry-oriented research funding, the deficient results of that struggle are well reflected in the relatively low competitiveness of Polish research and student training. Polish universities still fail to present themselves as hubs for innovation and knowledge resources for the industry.

The enhanced social security agenda, reflected in the country's budget, adds to the challenge of fueling innovation. When compared to Israel, who favours entrepreneurship, the recent social policy agenda in Poland, in particular the flag "500+ program", which focuses on social benefit directed at families with two or more children, the country has been criticized as supporting social dependency. While enhancing consumption in the near future, the social policy is also argued to represent a shortsighted labour policy, especially with regard to young women, who rely on social aid rather than seeking business or other professional opportunities. This complements a well-present post-communist syndrome of state reliance, with a growing group of socially dependent individuals, who reach out to the state for social security benefits rather than seeking business opportunities. Adding to that is the lack of a supporting mindset with regard to entrepreneurship, characteristic to Israel, with Poles perceiving business failure as reflective of individual shortcomings rather than a learning experience. Moreover, the post-socialist approach is well visible also in business, where it often views the state as a competitive actor and praises those who successfully manage to avoid state induced duties and obligations (tax, social insurance etc.), resulting in Poland having one of the EU's largest VAT revenue shortfalls.

[19] *Developments In Individual OECD And Selected Non-Member Economies. Poland*, OECD, accessed on: 26th of October 2017, available at : http://www.oecd.org/eco/outlook/economic-forecast-summary-poland-oecd-economic-outlook-june-2017.pdf

[20] CWUR World University Rankings – 2017, CWUR, accessed on: 26th of October 2017, available at: http://cwur.org/2016/poland.php. Israel's top universities rank at 27th, 39th, and 87th place respectively.

Tab. 1. Top CWUR universities in Poland and Israel (2017)[21].

World Rank	Institution	National Rank	Quality of Education	Alumni Employment	Quality of Faculty	Publications	Influence	Citations	Broad Impact	Patents	Score
27 **Top** 0.1%	Hebrew University of Jerusalem	1	16	217	15	133	119	278	168	37	59.12
39 **Top** 0.2%	Weizmann Institute of Science	2	21	616+	21	282	71	234	162	35	54.75
87 **Top** 0.4%	Tel Aviv University	3	72	82	53	109	122	183	146	45	49.61
421 **Top** 1.6%	Jagiellonian University	1	383+	616+	240+	407	416	482	356	299	43.49
464 **Top** 1.7%	University of Warsaw	2	110	517	153	461	414	415	455	673	43.30
666 **Top** 2.4%	Warsaw University of Technology	3	362	548	240+	737	768	302	621	862	42.84

These general social circumstances strongly differ from those in Israel, add to the cybersecurity policy shortcomings and are reflective of Poland's general economic condition.

Cybersecurity policy and competence

Distribution of cybersecurity competences in Poland has always been a complex matrix. Despite enhanced efforts of three consecutive governments, with the last two representing strictly opposing political views, the struggle over cyber resilient competences continues.

It was in 2008 that the Polish authorities took it upon themselves to develop a national strategy for cyberspace protection in Poland, which was to serve as a basis for an effective and systemic rise in the information security of the state. Since 2008 the then Ministry of Interior and Administration and the Agency for Internal Security (Agencja Bezpieczeństwa Wewnętrznego, ABW) attempted to set up a comprehensive, national cybersecurity strategy. Effectively, in the following three years seven strategic projects were presented:

- "Government Program for the Protection of Cyberspace of the Republic of Poland for 2008-2011" (November 2008);
- "Government Program for the Protection of the Cyberspace of the Republic of Poland for 2009-2011" (January 2009);
- "Government Program of Cyberspace Protection for the Republic of Poland 2009-2011" - (March 2009);
- "Government Program for Cyberspace Protection for the Years 2011-2015" (May 2010);
- "Government Program for Cyberspace Protection for the years 2011-2016" (June 2010);
- "Government Program for the Protection of the Cyberspace of the Republic of Poland for the Years 2011-2020";
- "Cyber Security Policy of the Republic of Poland" (May 2011).

None of these documents was approved by the Council of Ministers and executed. The policy documents failed to present precise objectives, meters or deadlines as well as institutions responsible for their execution. They lacked budgetary estimates,

[21] Based on data available at: http://cwur.org/2017

detailed and implementable action plans as well as sources of their funding. As a result, Poland spent several years on inter-ministerial arrangements of national strategy for cyberspace protection instead of looking for feasible solutions. According to the Polish Supreme Audit Office, authorities have been "focused on elaborating a poorly understood compromise between various public institutions".[22]

In 2013 the Council of Ministers adopted the Policy for the Protection of Cyberspace of the Republic of Poland[23] which deliberately focused on a very narrow perception of cybersecurity. It defined "cyberspace of the Republic of Poland" (CRP) as "cyberspace within the territory of the state in and out of its territory, where the representatives of the Republic of Poland are present (diplomatic missions, military contingents)"[24], making the duties and obligations applicable only to government administration, that is: 1) offices supporting the state bodies of government administration: the Prime Minister, the Council of Ministers, ministers and chairmen specified in statutes of committees; 2) offices supporting central bodies of government administration: other than the above-mentioned, i.e. bodies subordinate to the Prime Minister or individual ministers; 3) offices supporting local bodies of government administration: province governors, bodies of combined and non-combined administration 4) the Government Centre for Security.[25] Among others it introduced the cybersecurity plenipotentiaries responsible for reporting abuse to those specific, governmental online systems. It failed to address the complexity of state cybersecurity, in particular the cooperation between the private and public cybersecurity sectors, while noting that the majority of cybersecurity's vulnerable resources rests in private hands.

The latest cybersecurity policy, adopted by the government, is the 2017 National Framework of Cyber Security Policy of the Republic of Poland for the years 2017 – 2022.[26] It offers thus far the most comprehensive approach to cybersecurity, referring to, among others, the need to ensure public-private partnership with regard to cybersecurity, but following its predecessors, it fails to indicate the details of implementing the intended cybersecurity plan by giving more details on e.g. the timeline or funding. It does little to overcome the complex matrix of competing state authorities and the existing, uncomfortable power compromise between over a dozen governmental entities. It also fails to address the existing legal confusion, where numerous legal acts refer to individual cybersecurity challenges or sector specific tasks, lacking a coordinated approach.

There still are almost a dozen governmental entities entitled to manage cybersecurity competence and the Ministry of Digital Affairs, thus far indicated as the policy manages in all things cyber, has not been named as such in the 2017-2020 strategy document. Poland has no comprehensive legal framework nor an efficient policy mechanism to cater to its cybersecurity needs. The two key competing players have always been the **Ministry of Defence** and the **Ministry of Digital Affairs**, formerly operating as the Ministry of Administration and Digitalisation. However, all policy documents have bluntly referred to national laws entitling many other players to be consulted, supported or called to action in case of a cyber-emergency. The list traditionally includes, but is not limited to; the **National Security Bureau** (Biuro Bezpieczeństwa Narodowego, BBN), who is subjected directly to the President of the Republic; the **Internal Security Agency** (Agencja Bezpieczeństwa Wewnętrznego, ABW), which is responsible for, among others, countering internal espionage directly to the head of government; the **Government Centre for Security** (Rządowe

[22] For this critical assessment see: the 2014 audit report from the Supreme Audit Office, KPB-4101-002-00/2014, accessed on: 26th of October 2017, available at: https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf.

[23] Annexed to Resolution No. 111/2013 of the Council of Ministers of 25 June 2013 on the Policy for the Protection of Cyberspace of the Republic of Poland

[24] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Computer Emergency Response Team CERT.GOV.PL, accessed on: 26th of October 2017, available at: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html

[25] Idem.

[26] *Strategia cyberbezpieczeństwa przyjęta przez rząd*, Ministry of Digital Affairs, accessed on: 26th of October 2017, available at: https://www.gov.pl/cyfryzacja/strategia-cyberbezpieczenstwa-przyjeta-przez-rzad

Centrum Bezpieczeństwa; RCB) who advises the government on all strategic issues, including critical infrastructure protection; the **Ministry of Internal Affairs** which is responsible for, e.g. supervising parts of national critical infrastructure; the **Office of Electronic Communications** that regulates the telecommunications and postal markets; the **Ministry of Justice**, that introduces laws against cybercrime and terrorism; the **police** in all matters related to cybercrime or the **Ministry of Finance**, who controls banks, just to name the 10 key players. It's worth noting that the Ministry of Foreign Affairs, a very popular policy choice for coordinating all issues related to the Internet and its secure operations, has never been a major player in the Polish political cyber-realm. The original Polish idea was to create a central body, the Ministry of Digital Affairs, coordinating all policy issues related to the online environment – from online markets, through medial policies up to cybersecurity and resilience issues. Regretfully, neither the Ministry of Digital Affairs introduced in 2015, nor its predecessor – the Ministry of Administration and Digitalization, set up in 2011 have been able to live up to this centralized, optimistic scenario. This might be the case because the positioning of the cyber-policy within the competence of the local internal affairs regulator has been somewhat of a coincidence, not a well thought out policy decision – in early 2000s the Internet was perceived solely as a part of the physical telecommunications infrastructure, one traditionally subjected to this particular branch of government.

The legal matrix

The state fails to address the multi stakeholder nature of Internet governance not only by disregarding the need for a stimulated, enhanced private-public dialogue and partnership, but also by failing to ensure legal certainty and uniform implementation of the numerous legal acts targeting individual cybersecurity measures.

While still failing to introduce a comprehensive cybersecurity law (see further for the brief discussion on the current draft), the most notable provision in Polish law that targets cybersecurity, covers:

- » Articles 175 and 175c 1 point 1-2 of the Law on Telecommunication from July 16, 2004, which stipulates that telecommunication companies must take technical and organizational measures in order to ensure the safety and integrity of the network, services and communication (including, among others, elimination of the data that threatens the security of the network or service and interrupts the provision of telecommunication services) and inform users if they have been exposed to the risk of security breaches.
- » Article 7 (1) of the Act of July 18, 2002 on the provision of services by electronic means, which implements the e-commerce Directive, obliging service providers to prevent unauthorized access to the content of the communication they enable.
- » Article 50 sec. 2 of the Banking Law Act of 29 August 1997, on the basis of which banks must undertake special care in ensuring safety for the monetary resources that they hold in deposit.
- » Article 10 (1) (3) and 10 sec. 2 of the Act of 18 September 2001 on electronic signature implementing the duty to provide certification services for electronic signatures that include anti-counterfeit certificates and other data verified remotely, in particular by protection of the equipment and data used for the provision of certification services.

New laws and extralegal challenges

The proposed, yet not publicly available draft of **cybersecurity law** (the Act on the national cybersecurity system)[27] is aimed at implementing the NIS Directive. It therefore repeats much of its stipulations, yet fails to address its intended vagueness, such as the financial and technical measures for supporting businesses in implementing efficient cybersecurity, creating platforms for exchanging good practices and threat information or ensuring an effective domestic system for cybersecurity oversight. The proposed National Center of Cybersecurity (Narodowe Centrum

[27] Ustawa o krajowym systemie cyberbezpieczeństwa, draft dated July 10th, 2017, on file with author.

Cyberbezpieczeństwa) is yet another crossectoral body lacking effective competence to supervise offensive and defensive cybersecurity measures. It's Article 22 follows the lines of prior Polish antiterrorist laws, offering an access to cyber-surveillance to a broad range of bodies, including all the key players in the Polish cybersecurity game (Ministers of: Digital Affairs, Defense, Internal Affairs, Administration, Head of the Internal Security Agency, Head of the Governmental Security Center and the Head of the National Security Office). Despite European Commission's guidelines, the draft fails to define the "substantial impact of an incident", a term crucial to identifying a cybersecurity obligation on the part of the regulated bodies.[28] This is just to name a few of the shortcomings surrounding the timely implementation of the NIS Directive, crucial to a coherent European cybersecurity, which is set to be in place by mid-2018.

Recently first Warsaw School of Economics and then University of Warsaw launched Poland's post-graduate, yearly cybersecurity programs, based on a similar course led by Yale University's Cybersecurity program. It is focused on enhancing professional opportunities for security professionals and focuses on law, IT security, cybersecurity risk assessment, risk analysis, cybersurveillance, planning and security procedures. Earlier notable attempts at enhancing Poland's human resources in the cybersecurity sector include e.g. the 2013 launch of a cybersecurity and cryptography course at the Wroclaw University of Technology and an English course on Cyber Security Management at the University of Economy, also in Wroclaw.

These latest developments provide for an exemplary justification of Poland's governmental war over cybersecurity – only 2017 saw three strong attempts to centralize cyber-competence: from the Prime Minister's Office, Ministry of Defense and the Ministry of Digital Affairs, thus far vocal to any cybersecurity or Internet Governance imitative, currently clearly losing its pole position.

The developing situation regarding the cybersecurity in Poland makes the final chapter of the report – the comparison of the most important aspects of the cybersecurity systems' in Poland and Israel – even more important in the current debate and might be a needed step towards the broader view of the cybersecurity in Poland.

[28] COMMISSION IMPLEMENTING REGULATION (EU) laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

Chapter 3

Summary - a path forward - comparing Israeli and Polish experiences

Grzegorz Małecki

As proven in the two previous chapters, there is a wide range of differences in the Israeli and Polish systems of cyber security. Even though both states started developing the systems at a similar time, the state of the current affairs allow us to compare the different paths that the countries took while pursuing security in cyberspace.

The summary at the end of this report is to underline the main differences and present the possible solutions to the current debate within the administration in Poland, and to propose a way forward basing on the successful Israeli experience that is confirmed by the high level of security of the Israeli cyberspace.

The ecosystem of cyber security

What Israel excelled at was the creation of a cyber security ecosystem that consisted of a wide range of actors - both public and private, civilian and military, all of whom worked for the same goal – to create a well-functioning and well-maintained system of protection for the Israeli society.

While having only one governmental body to control and legally regulate the whole system is an important part of the Israeli success, the ecosystem is just as, or even more important. The cooperation between the private and public sector is based on the strong focus of the government to support the public education system, companies and start-ups, as well as to allow the influence of the army and intelligence services to participate in the system - not as the main actors, but as additional support.

The Israeli success story regarding their cyber security system was successful not only due to big investments and aids from the budget, but also because of the previous focus of the Israeli economy on the high-tech and the long-maintained focus of the Israeli society to provide technical education to a large percentage of the population. Several programs within Israel are focused on directing young people - both before and during the military service - towards technical knowledge like engineering, programming, computer studies and many others, making these field of studies not only interesting but also more profitable, convincing a large part of the students to undertake them. The Israeli Defence Forces not only allow the young people with the suitable education to broaden their expertise, they also have several courses for the soldiers to change their points of focus towards programming and software skills. Those young people join the workforce later on with a rather narrow expertise that allows them to focus on cyber security as one of the main fields.

Comparing the situation to Poland, Israel is much more invested in the promotion of technical studies, which results in a much more qualified workforce that, in turn, drastically improve the cyber security system. The workforce is one of the main elements of the well-functioning ecosystem and as such should be a major point of focus if a state is striving to become secure in the cyberspace. The lack of the well-trained workforce is not only the domestic issue of Poland, but the problem of the most of the European states.

An additional and important issue about the ecosystem is - apart from the legal regulations - it regulates itself. The cooperation between the public and private sector, once established, develops itself at its own pace. What worked so well in Israel is the cooperation between the public and private actors that allowed the joint budget to cover all the needed expenses.

The holistic approach and the one governing and regulating body

Another point to compare and to work on is the approach of the Israeli government to cyber security as a widely defined issue. The Israeli government understood well in 2010 that cyber security exceeds the field of competence of any existing at that point ministry and therefore instead of dividing the issue into a smaller fields of expertise that would suit the objectives of several administrative branches they decided to create a new body within the Prime Minister's office to address the whole issue. Not only did it suit the importance of the task well i.e. securing the Israeli cyberspace, but it also guaranteed that no conflict of interests will occur.

Currently, in Poland we have many actors who have some objectives connected to cyber security, but none of them are focused on the issue at large; rather establishing that only their part is assured. What Poland lacks right now is one major institution, and as the governmental structures are similar to the Israeli ones, in the Prime Minister's office, which will take care of the all aspects of cyber security in Poland - not only data protection but also military and civilian cyberspace defence, and the coordination of cooperation between the business sector and public actors.

Poland requires one governmental body that will focus on cyber security as a whole, and will treat the issue as a range of narrower tasks. The consolidation of the topic would lead to one institution being in charge of all the issues in regard of cyberspace, while other governmental actors - like the Ministry of Defence or the Ministry of the Digital Affairs - might still lead the efforts in particular topics like creating cyber defence units within the Polish army or the Homeland Security, creation of a well-established system of data protection, or ensuring that the European regulations regarding the cyber security would be properly implemented.

The additional problem that Poland is facing right now is the lack of a clear distinction of the responsibilities between the governmental entities that are to some point in charge of Polish cyber security. The Israeli system, in which one institution is in charge for all of the cyber security and the coordination of the actions of other governmental bodies, guarantees a clear distinction of objectives.

This lack of clear objectives within the Polish system of cyber security between the actors in the administration also leads to the lack of proper principles that would ensure a homogenous set of the laws. The creation of uniform directives and regulations that would be observed by all the actors in Poland could be a big step in the direction of a more effective cyber security system and could also cause all the governmental actions to be carried out with the regard to the same standards.

The suitable solution to the current situation will be the unification of the all the cyber security competences under the auspices of a new institution overseen by the Office of the Prime Minister, who not only has a vast and valid authority as a leader of the executive branch of the Polish government, but also is the only governmental institution that has a strategic overview of the broad range of the different issues that compose the current cyber security system - the Polish Prime Minister has, as the only institution in Poland, horizontal perspective in coordinating the budget of the widely understood cyber security and has possibilities to overlook the whole spectrum of the cyber platform. The strategic position of the Prime Minister, the creation of new structures in charge of cyber security in the authority of the Prime Minister's Office (in creating the new cyber security system in Poland) is vital to its success and might be the difference between founding a thriving new ecosystem and allowing it to fail due to the internal quarrels within the government.

Coordination between the public and private sectors - issue of financing

As mentioned before, there is very low level of coordination of the public and private sectors in regard of cyber security, which is especially visible when it comes to financing. In Israel the cost of the creation of the cyber security ecosystem was financed by the governmental budget, but the managing costs are divided in half between the government and the private sector.

Poland still lacks one institution within the government that will be in charge of its cyber security and due to that it also lacks a clear budgetary division of costs regarding the security of the cyberspace. The budget is realised by several public institutions and therefore it is somewhat difficult to assess the overall scale of the budgetary expenses to cyber security itself. Building on the Israeli experience, it might be useful for Poland to work out a similar way of division of the costs with the private sector, that will benefit from the possibilities to invest in cyber security and also benefit from the high security level provided by the state.

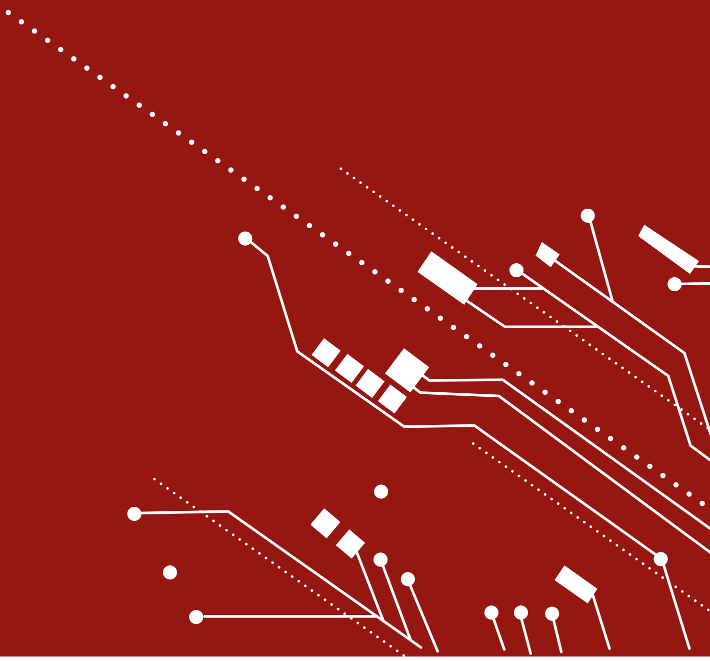
If, as we suggest, the Prime Minister's Office was in charge of the whole cyber security system, it would be much easier for the government to involve more ministries, which are currently uninvolved in cyber security, as they are not perceived as the key-assets to the cyber-strategy – the Ministry of Development, the Ministry of Science and Higher Education and many more. They have the capacity to make a difference regarding the creation of a well-maintained ecosystem. All of the important ministries in the government should take part in efforts and should be led by one strong leader - the Prime Minister - who can ensure the proper cooperation between the different actors of the executive branch.

A path forward for Poland

As visible in this brief summary, there are number of issues that were solved differently in Poland and Israel. Focusing on what lies ahead – from both the domestic and from the European perspective it is a further advancement of the cyber security. Poland should consider focusing its efforts on two major aspects of the Israeli success: the creation of a dynamic and self-managing ecosystem, that would involve as many private and reliable actors as possible to balance the financing of the system and to ensure its future development to counter the future threats, and the creation of one governmental agency that would be in charge of the cyber security issue as a whole - in our opinion it should be a specialized institution that would be launched under the authority of the Prime Minister, which would ensure its success and funding. The foundations for the process were laid down by the speech of Madam Prime Minister Beata Szydło in Cracow during the Cybersec conference, but they must be followed by a strategic decision to take responsibility for the launch of a new cyber security system that will involve creation of the aforementioned cyber security ecosystem. Ensuring the safety of the cyberspace was declared as one of the priorities of the Polish government and should be pursued as such, especially given the higher importance this holds with each passing year to NATO and European Union.

Both of the above in our understanding are the most important parts of the Israeli cyber security 'success story' and - as Israel remains the leader in ensuring security of its cyberspace - it might be useful to learn from its experience in the matter.

While the cyberspace consists of many threats to contemporary states, it also holds possibilities and chances to those countries, which can pursue the cyber security development as an economic goal and focus its industry on searching for the solutions to the emerging challenges. The case of Israel is an excellent example, as its economy is booming due to the high investment of the state on the cyber. This might be a chance for Poland as well, especially since the cyber is still an underdeveloped branch of the EU's Member States' economy.



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Fundacja im. Kazimierza Pułaskiego
posiada status partnerski przy Radzie Europy

Fundacja im. Kazimierza Pułaskiego
ul. Oleandrów 6, 00-629 Warszawa
tel.: 022 658 04 01
faks: 022 205 06 35
e-mail: office@pulaski.pl

www.pulaski.pl
ISBN 978-83-61663-11-9