Security through innovation
Cybersecurity sector as a driving force in the national economic development
Wiesław Goździewicz, Cyprian Gutkowski, Lior Tabansky, Robert Siudak
Editor: Dominik Skokowski
SECURITY THROUGH INNOVATION. CYBERSECURITY SECTOR AS A DRIVING FORCE IN THE NATIONAL ECONOMIC DEVELOPMENT

Wiesław Goździewicz, Cyprian Gutkowski, Lior Tabansky, Robert Siudak
Editor: Dominik Skokowski

THE KOSCIUSZKO INSTITUTE
The views expressed in this publication are those of the authors and do not necessarily reflect any views held by the Kosciuszko Institute and the publication partners. They are published as a contribution to public debate. The authors are responsible for their own opinions and contributions and do not necessarily support all of the opinions made by the other authors in the report.
## CONTENTS

Executive summary .................................................................................................................................4

*Between security and economy: the public sector as a driver of growth in the cybersecurity industry* — Cyprian Gutkowski ........................................................................................................9

*Cyber defence and beyond: the role of the military in the national cybersecurity* — Wiesław Goździewicz .........................................................................................................................19

*Innovation made possible: government-business cooperation national case studies* — Lior Tabansky ..........................................................................................................................29

*From source code to export: advanced private ICT sector as a crucial part of the national cybersecurity ecosystem* — Robert Siudak ....................................................................................................43

About Authors ........................................................................................................................................55
Cybersecurity is not only about cost. If built properly, it may also generate revenue for the country. A strong national cybersecurity sector does not only help protect the state, but it can also be an important export commodity and a driver of economic growth.

The national cybersecurity sector cannot thrive without an active involvement of the government in both the civilian and the military domain. From a meticulously designed and executed national cybersecurity strategy through adequate partnership mechanisms to proper R&D programme, the government should support the cybersecurity industry throughout this chain.

- **PPP investments are cheaper by 15-17% on average.**
- **5.6 PLN bn** ($1.4 bn) focused on cybersecurity
- **112** public-private partnerships (2009-2016)
There are countries which went down that road and they are already reaping the benefits of the rapidly growing global cybersecurity market.

Poland has the potential to join and profit from the exponential rise of this market. It has a strong ICT sector, adept workforce, and a thriving academic community.

Furthermore, Poland can benefit from its membership in the supranational organisations.

As a member of EU Poland can benefit from European Comission’s plan to invest EUR 1.8 bn by 2020 in cybersecurity industry.

As a member of NATO Poland can utilise such mechanisms as The NATO-Cyber Industry Partnership.
Cyberspace and threats arising from it are here to stay if we like it or not. It is up to us if we decide to benefit from it or fall behind.

However, in order to fully embrace the opportunity, Poland must undertake action. The key conclusions of the following report lead us to propose:

DEVELOPING PUBLIC-PRIVATE COOPERATION MECHANISMS
- adapting the existing public-private cooperation mechanisms to include cybersecurity-oriented projects, e.g. the public-private partnership,
- seizing the existing opportunities for cooperation that stem from the Polish membership in NATO and the EU,
- creating new mechanisms, especially for dealing with emergency situations such as large-scale cyberattacks.

DEVELOPING MILITARY-INDUSTRY COOPERATION MECHANISMS
- developing methods of cooperation between the military and the private sector in times of war and peace,
- engaging skilled individuals for cyberdefence purposes,
- creating long-term partnerships between the Armed Forces and national ICT companies.

DEVISING A ROBUST R&D PROGRAMME
- providing grants,
- procuring R&D services from commercial partners,
- providing tax incentives for companies conducting R&D.

DEVELOPING MARKETS
- boosting the domestic cybersecurity market by making the central administration and state-owned enterprises more open to cooperation with national companies of all sizes,
- changing the legal framework to increase the competitiveness of national ICT companies (including startups and SMEs) in public bids,
- helping national companies access foreign markets by preparing and executing a long-term PR strategy to promote Poland as a cybersecurity centre of excellence.


5. The Institute for Public-Private Partnerships, PPP market analysis for the period from 2009 to 31 December 2016.


7. Israel’s National Cyber Bureau data.


Secure cyberspace is one of the most serious challenges of the modern world. It applies to all across the board, with no exception: the government and local administration, all the sectors of the economy, the ordinary citizens, even those who do not use a computer at all. The dynamics of the changes taking place in cyberspace makes it necessary to draw special attention to the need for enhanced protection of data resources. This protection should be structured and provide three basic security components, i.e. confidentiality, integrity and availability (the so-called CIA triad).

Any cybersecurity assurance activities must comply with the constitutional order established in accordance with the principle of law and the resultant accountability and competence of the relevant public authorities. We need to bear in mind, however, that the mere engagement of the state in creating systemic solutions and a legal framework to combat cyberthreats is simply not enough. What is required is the synergy between the state and the private sector. It is totally unacceptable for the public administration to impose various obligations and expectations on the private sector and at the same time have no competencies facilitating effective collaboration in their implementation. Cyber exercises carried out by the Cybersecurity Foundation - Cyber-EXE Polska,
2014 perfectly exemplify the problem. During the exercises, telecommunications operators were required to report security incidents to multiple authorities of the state administration. Unfortunately, they had trouble getting any support from these authorities to coordinate the crisis situation. For these reasons, it is necessary to build different models of cooperation between operators and public administration in cybersecurity as well as to develop good practices.

Building synergy through public-private partnership

One of the potential forms of effective cooperation between the state and private sector representatives is a public-private partnership (PPP). Although Poland has never applied the mechanism to cybersecurity projects, it has significant potential. From 2009 to December 2016 a total of 112 contracts
worth PLN 5.6 billion (USD 1.4 billion) were concluded under the public-private partnership. Unfortunately, none of them represents an example of cooperation to improve the cybersecurity of the civil public sector. We can only presume that cybersecurity is an element of some of these undertakings at best. The list of completed tasks includes projects related to the provision of broadband Internet services. However, there were only 13 projects like that, worth PLN 1.9 billion (0.5 billion USD), which stands for only 11.6% of all contracts. On the other hand, this makes up 34% of all PPP funds. However valuable and necessary from the point of view of country digitization, this initiative does not, strictly speaking, address the issue of security in Polish cyberspace.

By synergising the potential of the public entity and its private partner, a public-private partnership enables them to develop new infrastructures more effectively and efficiently as well as to improve the standard and efficiency of public service delivery. As far as the public administration is concerned, PPP in Poland is being implemented mainly by the local authorities who have managed to conclude 103 of 112 contracts (92%). Conversely, the government administration finalised only 5 contracts (4.5%) until the end of 2016. The dominant position of local governments determines the present shape of the PPP mechanism. Local governments are interested in the implementation of tasks at the local level, whereas cybersecurity must be seen far more broadly.

The benefits of PPP
- Lower public spending on investments, bringing savings to the budget
- Speeding up the construction of public utilities and the supply of related services
- Provision of higher quality public services
- Greater competitiveness of private capital in the public service delivery sector
- Investment risk-sharing between the public authority and the private entrepreneur
- Additional growth prospects for private companies

The benefits of “ad hoc partnership”:
- Flexibility in determining the terms and conditions as well as the formula of cooperation
- Smooth allocation of specialists in the event of a crisis situation
- Cost-effectiveness
- The development of good practices
Employing the PPP mechanism in the field of cybersecurity could bring many benefits. First, in contrast to typical privatisation of public services, the PPP model leaves the responsibility for the quality of service delivery with the public administration by only outsourcing the actual execution of the task to private entities. In the case of such a sensitive issue as the cybersecurity of state resources, this constitutes a key factor allowing the public administration to retain the necessary degree of authority over the realization of a privatised public task. Second, the PPP investments are cheaper by 15-17% on average. In addition, implementation delays in PPP schemes are less common compared to public projects carried out by the public administration. They are also far more likely to stay on budget.

Beyond strategic documents: flexible forms of cooperation

A public-private partnership on secure cyberspace cannot be understood in purely statutory terms, i.e. as cooperation between government authorities and local governments (public administration) and private actors based on long-term agreements made to develop infrastructure components to enable the provision of public services. This collaboration should result in establishing good practices, including the exchange of information and cooperation with the business community in the event of a cyberthreat not provided for in agreements. After all, the innovation in information and communication technologies (ICT) simultaneously strengthens the arsenal of cyber criminals and expands the threat landscape itself. It is therefore impossible to enumerate all cybersecurity-related aspects in an exhaustive list in a typical cooperation agreement between the civil public sector and the private sector. Creating solutions that allow for tapping into the pool of professionals in the private sector becomes particularly essential in the event of a sudden, isolated, yet extremely dangerous incident jeopardising the country’s critical infrastructure and requiring rapid expert support for state human resources.

Private-sector wages in the area of cybersecurity are 20% higher on average than those in the public sector. The proposed ad hoc public-private partnership reduces the identified pay gap, allowing private sector professionals to gain unique experience.

It is difficult for the public administration to compete with the private sector for highly skilled cybersecurity professionals. According to the SANS Institute, private-sector wages in this area are 20% higher on average than those in the public sector. Similarly, according to research by the
Central Statistical Office of Poland (GUS), IT professionals in state agencies earn about 33% less than their counterparts in private companies.6 The proposed ad hoc public-private partnership reduces the identified pay gap, allowing private sector professionals to gain unique experience and ensure that state resources have an optimal level of cybersecurity. A similar solution has been employed in Estonia, where under the public-private partnership private sector volunteers are to support public administration personnel in the state of emergency. This is discussed in greater detail in the next chapter. It needs to be noted that a small country like Estonia has spent EUR 16 million (USD 17.5 million)7 on the implementation of its cybersecurity strategy in the years 2014–2017. Adapted to Polish circumstances, the ad hoc public-private partnership could provide a significant help for the state in a time of crisis and protect the country’s critical infrastructure from a sudden and dangerous incident. It is worth adding that Poland has also set up a similar structure “Polish Civil Cyber Defense Association”, which gathers experts (ranked 3rd in 114 in Cyber Europe 2016 exercises) ready to serve the state.

Public-private cooperation: Polish experience

An interesting example of cooperation is the National Cybersecurity Centre (NC Cyber), launched as part of the Research and Academic Computer Network (NASK) and designed to ensure the security of cyberspace of the Republic of Poland through the development of national ICT security plans. NC Cyber acts as an early warning centre which monitors and administers the reporting mode on network threats. The centre also manages a hotline for reporting harmful and illegal content. A number of private security actors have acceded to the agreement under NC Cyber, including Citi Handlowy, Credit Agricole, mBank, PKO BP, Raiffeisen Polbank, BZWBK, Orange, T-Mobile, Polkomtel, Energa, PSE S.A., Gaz-System S.A., PERN S.A. and PKP Informatyka.

Cybersecurity Forum founded in December 2016 at the Ministry of Digital Affairs is an advisory body assigned to diagnose the needs and set priorities for joint action by all stakeholders in the national cybersecurity system.

The next convenient formula of public-private cooperation is the Cybersecurity Forum at the Ministry of Digital Affairs. Founded in December 2016, this advisory body has been assigned to diagnose the needs and set priorities for joint action by all stakeholders (within the framework of the so-called broad public-private partnership) in the national...
cybersecurity system. The Forum has also established expert groups working on specific topics. One of them, namely NC Cyber development team, is particularly interesting from the point of view of fostering cooperation with the private sector. On the one hand, grouping strategic stakeholders will help gain knowledge about what is expected of NC Cyber, and on the other hand, it will provide an opportunity to offer preferred means of information exchange and collaboration.

Trusted Profile (Profil Zaufany) is another example of successful cooperation between the private sector and the public administration. The project initiated by the Ministry of Digital Affairs enables the use of the Electronic Platform of Public Administration Services (ePUAP) and gain electronic access to public services. Electronic banking allows the citizens to obtain their individual Trusted Profile, in other words get their identity confirmed by means of their bank account, which subsequently allows them to access public services over the Internet. A similar cooperation model was used in the programme “Family 500 plus” where the bank was held responsible for verifying the applicant and protecting them against risks such as identity theft.

According to the Ministry of Family, Labour and Social Policy, 20% of nearly 3 million applications for the programme were submitted online, while a total of 18 banks reported their readiness to participate in the project.

Public-private cooperation in light of the National Cybersecurity Policy Framework

So far all cybersecurity activities undertaken by public and private sector entities and institutions responsible for countering cybercrime were largely dispersed, which contributed to the low efficiency of the entire system. Currently, in accordance with the National Cybersecurity Policy Framework of the Republic of Poland in the years 2017–2022, these actions are to be consolidated and harmonised. In this document, the government responds to other challenges such as investing in the expansion of industrial and technological cybersecurity resources by facilitating the development of enterprises, startups, and R&D centres that create innovative solutions for cybersecurity. All actions for the development of national capacity and competencies have been given the status of

The European Commission in collaboration with the European Cyber Security Organisation (ECSO) have launched the contractual public-private partnership on cybersecurity. It aims to boost cybersecurity investments in the EU, which are expected to reach EUR 1.8 billion by 2020.
strategic objectives. To date, the implementation of these tasks has been viewed only in technical terms or as a means necessary to execute tasks within the cooperation for innovation framework or a public-private partnership. As it stands, the development of domestic product and service resources, support for R&D and public-private cooperation have been deemed strategic assets, recognising that they can become Poland’s national speciality and export commodity.

Another development programme under completion is the Cyberpark Enigma which envisages the recreation and enhancement of competencies in the production of hardware and software used by all industries. In addition, it has been appointed with the task of acquiring new technologies to foster the growth of domestic undertakings. According to the National Cybersecurity Policy Framework of the Republic of Poland 2017–2022, the implementation of this programme will not only strengthen Poland’s resilience to cyberthreats, but it will also provide an important stimulus for growth that will help Polish companies to compete in the European market of specialized ICT products and services.

Public-private partnership: European approach

On 5 July, 2016, the European Commission in collaboration with the European Cyber Security Organisation (ECSO) have launched the contractual public-private partnership on cybersecurity. It aims to boost cybersecurity investments in the EU, which are expected to reach EUR 1.8 billion by 2020. This objective is meant to be achieved by appropriately allocating EUR 450 million of European funds available under the EU Research and Innovation Programme “Horizon 2020”. The contractual public-private partnership on cybersecurity brings together business representatives (both large corporations and SMEs), national, regional and local authorities, and research and academic centres.

The partnership should also contribute to consolidating the single digital market in the area of cybersecurity. At present, in accordance with the treaty-based order, the primary functions of the state are aimed at maintaining public order and the protection of national security (also in cyberspace). The consequence of this state of affairs is various restrictions of free market freedoms or competition, for instance a scant participation of companies in public procurement outside the country of origin of the company. This fragmentation of the EU market strengthens the dominance of non-European players (the U.S. and Asia). In view of the above, a wide array of activities are planned for the consolidation of the single digital market in the field of cybersecurity, such as certification, validation (including the entire ICT sector), marking (quality and security/privacy mark), and a set of common specifications for tenders and regulation.
Good practices as an essential component of the national cybersecurity ecosystem

It is necessary to develop and adhere to good professional practices in public procurement, tendering, or the selection of cyber service subcontractors in large public institutions like the Social Security Office (ZUS), the Inspector General for Personal Data Protection (GIODO), the National Health Fund (NFZ), etc., or other state-owned companies of strategic importance. The state should develop such a legal framework, entrusting cybersecurity to only verified and reliable entities. The price should by no means be the determining factor. Far more important are the trust and confidence in the selection of the right partner to properly complete the assignment. Negligence or letting unauthorized entities handle ICT security may in effect put the security of the state in jeopardy.
Sources:
1. All conclusions from the exercise can be found in the report Cyber-EXE Poland 2014, [online] https://www.cyberexepolska.pl/wp-content/uploads/2015/01/CYBER-EXE2014_RAPORT-PL.pdf (access: 12/05/2017).
2. Based on the report by the Institute for Public-Private Partnerships, PPP market analysis for the period from 2009 to 31 December 2016.
Cybersecurity is a multi-faceted and cross-sectoral phenomenon that requires the involvement of the various sectors – military, civil, public and private – to counter all foreseeable threats.

It is also an area in which there is a possibility and a vital need to engage with both the industrial sector and academia as the potential suppliers of modern software and hardware solutions. There are companies in the world specialised in providing state customers with cyber tools, including the offensive ones.

As part of a more broadly understood concept of information security, cybersecurity will interpenetrate other domains, including the physical security of the network infrastructure. Cybersecurity is not possible without ensuring secure communications channels, including classified (secret) communications, and properly secured ICT networks – both confined, isolated from the Internet, and those connected to the Internet. In the latter case, effective safeguards are particularly important, such as data diodes controlling the flow of data between a protected network and the Internet.

Versatile cyber capabilities

Obviously, cyber defence capabilities must include passive measures protecting military ICT infrastructure (or the part of the civilian ICT infrastructure used for military purposes) from unauthorized access or even hostile activities intended
to disrupt military ICT systems. They must also comprise measures enabling the secure and encrypted exchange of information between authorised network users. It is in the interest of the Ministry of Defence to ensure that the systems protecting the military network from unauthorized access or attempts to break into these networks as well as encryption algorithms are unique solutions, relying on commercial products to the minimum extent possible.

Regardless of the domain, effective and robust defence requires the availability of offensive measures in order to run active defence operations and launch counter-attacks, or retaliatory “hacking” (“hacking-back”) of the opponents’ systems and, if necessary, to launch a pre-emptive cyberattack.

Poland admits more or less openly to seeking offensive cyber capabilities.1 In 2013, the National Centre for Research and Development in Poland announced a competition for "Developing software and hardware solutions for conducting information warfare [...]" including "[taking over] control over network devices [...] and [the disintegration of] communication nodes by deliberately changing their operating parameters or deactivating selected functions." Further, we read that "[i]n order to take over components of the enemy’s network, it is necessary to install software (malware) and electronic equipment either openly or covertly [...]" and, that "[...] creating one’s own military botnets [...]" was being predicted.2

The estimated value of this project was over PLN 6.5 million (USD 1.7 million).

Commercially developed malware FinFisher is said to be used by intelligence agencies in several countries, allegedly including the Czech Republic and Slovakia.3 Furthermore, the German secret services are believed to have been using commercially delivered malware R2D2 for several years.4

The Technical Modernisation Programme (TMP) of the Polish Armed Forces for the years 2017–2022 stipulates that the Polish
army will allocate 1% of the total TMP’s resources, which amounts to approximately PLN 1 billion (USD 0.3 billion) in total, to the development of its cyber capabilities in the period 2017–2019, as well as throughout the five-year period covered by the TMP. Although this figure looks impressive nominally, it pales in comparison with the funds designed for other priority programmes, such as the modernisation of air defence, for which the Polish Ministry of National Defence intends to allocate 14% of the TMP’s value in the years 2017–2019, and a total of 24% in the entire five-year period. For the development of mechanised and armoured infantry, the Ministry is planning to allocate 14 and 20% respectively.5

Strengthening the military in cyberspace: cooperation and commercialisation

Building effective cyber capabilities requires broad cooperation of the Ministry of Defence and the Armed Forces, both with national and international partners. It is necessary to establish mechanisms for coordination and the exchange of information with civilian authorities and entities engaged in the country’s cyber defence, including the private sector, most notably the operators of critical infrastructure systems.

The importance of such cooperation has been appreciated by many states. For example, Estonia’s Cyber Security Strategy 2014–2017 provides for the creation of conditions to facilitate the organisation and provision of cybersecurity training, workshops and research, as well as to intensify cross-sectoral activities. In addition, given the mutual dependencies and connections (including physical networks) between infrastructure and ICT services, this document recognises that the cooperation among public, private, and academic sectors is essential to building cybersecurity in a coordinated manner.6

The French digital security strategy formulates similar theses, but it goes a step further by suggesting, just like the present study, that it is necessary to promote the competitiveness of the domestic cybersecurity industrial and research sectors in order to ensure national digital sovereignty. France is committed to fostering innovation and a research-friendly environment by mobilising and coordinating all available public and private resources to give French cybersecurity solutions competitive advantage, which in effect will tangibly benefit both the private sector and the state.7

Possible directions for military-industrial cooperation

The cooperation between public, private, and academic sectors may considerably reduce the duration of research and development work, provided that appropriate information exchange and sharing mechanisms are created in the first place.
NICP can serve as a model for cooperation with academia and the industrial sector. The partnership is based on a legitimate assumption that close cooperation between the contracting authority (NATO) and the supplier (the industry) is the key to streamlining cybersecurity solutions, while the inclusion of the academic sector in this cooperation will grant access to the latest achievements in science and technology.

The NICP brings together NATO institutions, national CERTs and industry representatives of NATO Member States, including medium- and small-sized ICT companies, as well as academic centres. Facing common cybersecurity threats and challenges, all these actors share the belief that cooperation and exchange of information, notably with regard to the latest R&D solutions developed by private business and research centres, can significantly accelerate NATO’s efforts to develop robust cyber defence capabilities.8

As part of the NICP framework, the NATO Communications and Information Agency (NCIA) has created Information and Cyber Incident Coordination System (CIICS), the development of which was contracted to the Rhea Group, the Belgian subsidiary of the Canadian ADGA Group.9 With an annual budget of EUR 600 million (USD 657.3 million) for ICT infrastructure projects,10 the NCIA is planning to spend between 2016 and 2019 a total of about EUR 3 billion (USD 3.3 billion) on a variety of ICT projects in support of command and control systems as well as satellite communications, air defence, and cyber defence systems.11

Within the NICP framework (see NICP case study), such mechanisms function on the basis of Industry Partnership Agreements (IPAs) that the NCI Agency concludes with the industrial sector. The Agency has entered into such agreements with FireEye or RSA Security, to name just a few. The aim of the IPA is to allow for rapid exchange of information on cyber threats in order to improve the situational awareness of the parties to the agreement and to strengthen the protection of their networks. Mutual benefits yielded by the cooperation among the military, industrial partners and academia are not to be underestimated, especially when this cooperation is extended to include national entities. It will:

- enable domestic companies and academic centres to obtain R&D funding to develop solutions requested by the Ministry of Defence.
- allow for customising the solutions being developed by the industry
• help increase the security of the designed solutions and systems.

Relying on national entities in the industrial and academic sectors to develop cyber capacities, particularly cryptanalytic and cryptographic solutions, will help create truly secure products and services. This can be done by drafting the terms and conditions of the procurement in such a way as to oblige the author of the solutions to make the contracting authority the sole recipient and user of the source codes and solutions they create. The most important aspect here is to become less dependent on widely available commercial products that are often riddled with security vulnerabilities, in some cases left there deliberately by the manufacturers, as was the case with the RCS system purchased by the secret services in a number of countries, including the Polish Central Anti-Corruption Bureau. Authors of commercial solutions reluctantly

and academic sectors to the specific needs of the contracting authority.

• help increase the security of the designed solutions and systems.

Examples of Cyber Defence Procurements Include:

- The implementation of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC); contract worth EUR 134,353.77 (USD 147,190.36) was awarded to SELEX Communications SpA;
- The implementation of the NCIRC interface at Ramstein missile defence unit; contract worth EUR 411,173.64 (USD 450,458.50) was awarded to SELEX Communications SpA;
- The installation of the Active Network Electronic Security System – ANWI ESS for NCIRC; contract worth EUR 352,166.22 (USD 385,813.32) was awarded to SELEX SpA;
- TrendMicro license renewal for NCIRC; contract worth EUR 101,481.02 (USD 111,176.84) was awarded to Insight Technology Solutions Belgium Inc.;
- McAfee license renewal for NCIRC; contract worth EUR 498,627.34 (USD 546,267.80) was awarded to UNI BUSINESS CENTRE B.V.;
- The central purchase of TEMPEST level B workstations; contract worth EUR 1,662,375.58 (USD 1,821,204.31) was awarded to Airbus Defence and Space AS;
- The purchase of communications and IT equipment for the NATO Force Integration Units – NFIUs; contract worth EUR 2,762,779.00 (USD 3,026,743.82) was awarded to Airbus Defence and Space AS;
- The purchase of cryptographic equipment for NATO’s communication infrastructure; contract worth EUR 941,334.89 (USD 1,031,273.06) was awarded to Thales Norway AS.
(if at all) grant their customers access to the software source codes, and often sell them as the so-called “black box” that allows for no user modifications or enhancements. The lack of access to source codes can effectively render the identification and elimination of potential security vulnerabilities impossible.

**Recruiting cybersoldiers: manpower shortage**

It is impossible to think of building cybersecurity potential without harnessing national human capital. The military structures will “own” this human capital only to a limited extent – the vast majority of cybersecurity experts will be absorbed by the civil sector, where the demand for these professionals is virtually unlimited. It is therefore necessary to create systemic solutions to either attract professionals to state institutions, including the military, or to put them under mobilisation assignment programmes to be deployed in the event of a crisis or an armed conflict, when strengthening the state’s defence capabilities, including cyber military capabilities, becomes absolutely critical. Examples of such solutions can be found in France where Cyber Civic Reserve (Reserve Citoyenne Cyber)\(^{13}\) has been launched or in Estonia, where the Cyber Defence Unit of the Estonian Defence League has been incorporated into the national defence system, giving the entire Estonian Defence League the status analogous to that accorded to the Armed Forces of Estonia in the event of an armed conflict.\(^{14}\)
Israel stands at the opposite extreme. To date, its defence forces are based on general conscription, which also includes women. Set up to conduct cyber operations, Unit 8200 brings together experts being both professional soldiers and conscripts. When asked about the human capital and the pay gap between the officers and non-commissioned officers and privates engaged in cyber operations, the former head and architect of the unit, Brig. Gen. Danny Bren said that the main motivation behind the decision to remain on active duty in Unit 8200 is after all the desire to face the challenges the service offers.\

Certainly, such solutions will also require an appropriate training system to be created in order to enable these civilian specialists to phase in relatively smoothly and get accustomed to operating in hierarchical state structures. One of the possible solutions is to announce volunteer "conscription" of professionals to participate in military and civilian crisis management exercises and trainings. Taking into account the salary ranges in the Polish Ministry of National Defence, it is quite safe to assume that in most cases civilian specialist will not consider the financial incentive as the main factor when taking decision to engage in activities to strengthen national cybersecurity. In accordance with the provisions of the Collective Labour Agreement for Employees of Military Budgetary Sector Entities, the maximum salary of the Ministry civil service personnel is PLN 8000 gross (USD 2083.82). However, it is highly unlikely that cybersecurity professionals will earn the highest salary given the hierarchical structure of civilian posts in the Ministry of National Defence.

The Israel Defense Forces scout universities for young candidates who have exceptional analytical skills and at the same time can work as true team players to serve in Unit 8200. As part of the compulsory military service, instead of learning the drill, weapon handling or tactics, successful candidates undergo training in Unit 8200’s comfortable, air-conditioned facilities where they learn how to collect intelligence, use state-of-the-art electronic surveillance or data mining techniques. The skills acquired in training have also helped ex-8200 soldiers to succeed in the commercial market. They are the masterminds behind establishing such companies as Check Point, CloudEndure, CyberReason, ICQ, LightCyber, the NSO Group, Palo Alto Networks, indeni, NICE, AudioCodes, Gilat, outrbrain, Leadspace, EZchip, Onavo, Singular, CyberArk or Fortscale. The Israeli army has heavily invested in its professionals who, capitalising on the knowledge gained in Unit 8200, have often succeeded in commercial cybersecurity business. They remain allocated to mobilisation assignment programmes, and are regularly called up for reserve training during which they can use their knowledge and experience gained both in military service and subsequent business activity.

The emoluments for reservists who are called up for military exercise do not look particularly attractive either. The net salary for a 30-day
exercise amounts to PLN 2100 (USD 547) for a private, PLN 2512.50 (USD 654.45) for Master Corporal, and PLN 3150 (USD 820.50) for Second Lieutenant. Lieutenant Colonel of the reserve can receive about PLN 5600 (USD 1458.68) for a 30-day exercise, whereas his German counterpart about EUR 3500 (USD 3834.40) plus extras for possessing qualifications and skills particularly useful for the army. The salaries offered by the Polish Ministry of National Defence are hardly competitive compared to the private sector offerings, which was repeatedly emphasized (also by the representatives of the Polish government) at the Polish Cybersecurity Forum in 2016 and the European Cybersecurity Forum in 2015.

An option worth considering is to search for specialists of the young generation who stand out in various competitions or hackathons, thus confirming their knowledge and skills that may be useful from cybersecurity perspective. Increasing the number of such initiatives, both nationally and internationally, is paramount to effectively address the problem.

In order to maximally utilise the human capital, without “pulling it out” of the work environment, cooperation with cybersecurity entrepreneurs willing to share their potential to enhance the state’s cyber defence capabilities should be considered. Such cooperation could include participation in dedicated cyber defence exercises. There have been cases of entrusting private companies with conducting security checks, including penetration tests of the ICT systems owned by ministries of defence. Another scenario to consider is to utilise the potential of companies and entrepreneurs associated in organisations similar to Polish Civil Cyber Defense Association, both by involving them in intersectoral and interministerial cybersecurity exercises and requesting them to conduct penetration tests or simulated cyberattacks on key ICT systems. These entrepreneurs could be engaged in developing effective methods and techniques to secure critical ICT systems by tapping into their experience in repelling cyberattacks on their own systems.


11. NATO announces 3 billion EUR investment in defence technology, 2016, [online] https://www.ncia.nato.int/NewsRoom/Pages/160726_Announcement_3billion_investments.aspx (access: 11/05/2017).


As the environment evolves at Moore's Law speed (overall processing power for computers doubles every two years), effective cybersecurity requires innovation that transforms the current practices and processes. Innovation generally arises from research and development (R&D), which comprises:

INNOVATION

While the business sector performs the vast majority of applied research and experimental development in ICT, academia engages predominantly in basic research. Innovation, however, largely hinges upon the cooperation among all these...
actors: the government, business, and academia. Having originated in economics and management in the late 1980s, the National Innovation System (NIS) concept allows us to analyse the entire range of stakeholders and interactions between them.\(^2\) A common proxy for innovation is to measure expenditure on R&D as a percentage of Gross Domestic Product (GDP).

This chapter analyses three case studies of Government-business Cooperation in Innovative National Cybersecurity Strategies: Israel, the UK, and Singapore. These three countries are ranked among the top 10 in innovation (5\(^{th}\), 8\(^{th}\), and 10\(^{th}\) respectively), with Israel and the UK considered world class powers, thus providing a useful reference point for Poland ranked 25\(^{th}\).\(^4\)
ISRAEL: HOW TO BECOME A WORLD-CLASS CYBER POWER IN 5 YEARS

Israel has emerged as one of the leading global cyber powers in recent years.\(^5\)

Since 2014, over 100 new cybersecurity companies have sprouted up in Israel, with 78 of them attracting nearly USD 400 million of investment in this period. At the government assembly held on 15 February 2015, the head of Israel National Cyber Bureau (INCB) stated that the Israeli cyber industry made record achievements in 2014.

- Approximately 30 early-stage cyber firms raised over USD 200 million – a 40% increase over 2013.
- Eight Israeli cyber companies were purchased by foreign investors for an overall sum of approximately USD 700 million.\(^6\)

Exports by Israeli companies in the cyber field 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 rose to USD 6 billion in 2014, second only to the U.S., and three times higher than the target the UK set for 2016.\(^7\) Israel currently attracts some 15–20% of global commercial cyber R&D investment. Counting 3,100 to 4,200 active tech startups, this makes Tel Aviv rank fifth in the world for best startup cities, the first outside the U.S.\(^8\)
The National Cyber Initiative was the expert committee which Prime Minister Netanyahu tasked in 2010 with a review of cybersecurity and Israel’s policy. The key question the committee scrutinised was how to incentivise and develop cyber technology in Israel, so it ranks among the top five world leaders by 2015.9

The bottom line of the recommendations made by 80 experts from all sectors working in 8 subcommittees for 6 months was to boost collaboration in the Israeli ecosystem involving the government, defence, academia, and industry.

The Government Resolution No. 3611 of August 7, 2011 ‘Advancing National Cyberspace Capabilities’10 accepted the National Cyber Initiative’s recommendations, becoming Israel’s public National Cybersecurity Strategy.

Stressing the need to advance cyber R&D, the new Israel National Cyber Bureau (INCB) was tasked with:

- promoting research and development in cyberspace;
- boosting the cyber industry in Israel (based on exports).

As of Q1 2017, five universities established Cyber Research Centres supported by the INCB. Inaugurated in September 2014, Tel Aviv University’s Blavatnik Interdisciplinary Cyber Research Centre (TAU ICRC) is the first institutionalised Israeli government-academia partnership in cyber-related research. The INCB funds nearly half of the research budget, but the fund allocation is institutionally independent and guided by the standard academic criteria of research excellence.

To improve the defence of national infrastructures essential for maintaining a stable and productive life in the State of Israel, and to strengthen those infrastructures against cyberattack by advancing Israel’s status as a centre for the development of information technologies while encouraging cooperation among academia, industry, and the private sector, government ministries and special bodies.

The Government Resolution No. 3611 of August 7, 2011, Advancing National Cyberspace Capabilities recommendation
The government refrains from commanding innovation processes. In addition to science and engineering, TAU ICRC also conducts policy research and public outreach.

The government via the INCB coordinates the development of the cyber industry, with the main project being the establishment of an additional cybersecurity cluster in Be’er Sheva co-locating the government CERT, military intelligence and technology units, the Ben Gurion University, and businesses. As part of the Be’er Sheva project, 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 in order to attract companies to set up their business there.¹¹
The UK published its National Cyber Security Strategy in November 2011, just after Israel did. The UK Strategy addressed economics, not only security, setting a target of GBP 2 billion (USD 2.6 billion) cyber security exports to be reached by the end of 2016. In collaboration with industry, academic and international partners, this 2011-2016 Strategy achieved tangible progress.

- In critical national infrastructure protection, government worked together with owners and operators, putting plans in place for managing cyber risks.
- Businesses of all shapes and sizes can receive unprecedented levels of government-supported expert guidance and training to help them manage their cyber risks, such as the Cyber Essentials scheme.

### THE UK CYBER SECURITY STRATEGY 2011-2016: SPENDING BY THEMATIC AREAS OF WORK

- National Sovereign capability to detect and defeat high end threats
- Law enforcement and combating Cyber Crime
- Support to full spectrum effects capability
- Private sector engagement and awareness
- Improving and resilience of the Public Sector Network
- Mainstreaming cyber throughout Defence
- Education and skills
- Incident management/response and trend analysis
- International engagement and capacity building
- Programme management, coordination, and policy
The Objective 7.2.3. of UK National Cyber Security Strategy 2016-2021

- provide testing facilities for companies to develop their products, together with a fast-track form of assessment for the next generation of cyber security products and services as they emerge, enabling customers to be confident in their use;
- draw on the collective expertise of the industry-government Cyber Growth Partnership to help shape and focus further growth and innovation interventions;
- help companies of all sizes scale-up and access international markets

- UK cyber security companies have increased their global market share.\textsuperscript{15} The UK domestic cyber security sector has grown from GBP 10 billion (USD 13 billion) to over GBP 17 billion (USD 22 billion), giving employment to 100,000 people. As a result, the market share of the UK’s cyber security exports grew from 3.6\% to 4.4\%, which amounted to GBP 1.47 billion (USD 2 billion) in 2014 – up by 35\% since 2012.\textsuperscript{16}

The industry has been involved in various roles throughout the thematic areas of work depicted.\textsuperscript{17}

The subsequent UK National Cyber Security Strategy 2016-2021 also dedicates significant attention to the government-business cooperation, such as the creation of a growing, innovative and thriving cybersecurity sector.\textsuperscript{18}

London is already ranked sixth in the world for best startup cities. In addition to supporting the clustering of high-tech companies, HM Government defines success in developing the business sector as:

- ‘greater than average global growth in the size of the UK cybersecurity sector year on year’ and
- ‘a significant increase in investment in early stage cyber companies.’\textsuperscript{19}

HM Government supports fundamental research in 13 Academic Centres of Excellence in Cyber Security Research (ACE-CSR) established at UK universities.\textsuperscript{20} Moreover, it stimulates companies of all sizes to join CyberInvest, an industry-Government partnership in order to invest in academic research.\textsuperscript{21} ‘Minimum investment levels range from GBP 10k (USD 13k) for ‘micro’ companies (companies with less than 10 employees) to GBP 500k (USD 650k) for large
companies (over 250 employees), with 24 companies having already committed to invest a minimum of GBP 8 million (USD 10.5 million) over the next 5 years via CyberInvest.

The most recent development in the process of strengthening the UK’s national cybersecurity system is the establishment of a new technical authority for cybersecurity – the National Cyber Security Centre (NCSC). The NCSC is part of the Government Communications Headquarters (GCHQ) responsible for bringing together UK expertise in the field of cybersecurity in order to provide assistance and guidance to both public and private entities in accordance with a new, unified government approach to cybersecurity. The NCSC’s main tasks involve supporting critical services providers and critical infrastructure operators, responding and managing major computer incidents as well as the coordination of information sharing (by combining the best of government, industry and academic expertise). The NCSC runs the Cyber Security Information Sharing Partnership (CiSP) initiative for entities with their own networks to share information and discuss activity on their networks. Finally, the NCSC cooperates with the private sector to provide tailored advice and guidance for specific sectors – mainly the elements of the UK’s Critical National Infrastructure. The NCSC also participates in the CyberFirst programme that fosters the development of the UK’s next generation of cyber professionals.
SINGAPORE: ON THE PATH TO BECOME A SMART CYBER NATION

Cyber security is absolutely essential if we are to become a smart nation. You can’t have electronic medical records, you can’t have financial technology, you can’t have large databases with information that could be abused or misused, you can’t afford a breach of privacy. So the way I look at it, cyber security is the flip side of the coin of being a smart nation.

— Vivian Balakrishnan Foreign Affairs Minister and Minister-In-Charge of the Smart Nation Initiative

Singapore is the most globalized and connected economy, consistently ranked top in business freedom, market openness, and government integrity. Singapore’s gross domestic expenditure on R&D (GERD) as a percentage of GDP increased from 2.0% in 2013 to 2.2% in 2014. Of this, business expenditure on R&D (BERD) as a percentage of GDP increased from 1.2% in 2013 to 1.3% in 2014.

Singapore is ranked 10th in the world (and first in Asia) for best startup cities. The country strives to become a ‘smart nation’, which drives a more holistic perspective on cybersecurity:

In April 2015, Singapore established the Cyber Security Agency (CSA), a national agency under the Prime Minister’s Office and administered by the Ministry of Communications and Information (MCI). Over the course of a year,

PUBLIC INVESTMENT IN RESEARCH AND INNOVATION

- National Technology Plan 1995: $2bn
- Science & Technology 2000 Plan: $4bn
- Science & Technology 2005 Plan: $13.5bn
- Research, Innovation and Enterprise Plan 2015: $16bn
- Research, Innovation and Enterprise Plan 2020: $19bn

“...
CSA consulted representatives from over 50 government agencies, business and professional associations, private companies and academic institutions with the aim to develop the country’s Cybersecurity Strategy. In October 2016, Singapore launched its Cybersecurity Strategy that rests on four pillars: \(^{30, 31}\)

- **Building a Resilient Infrastructure**
  - Building a resilient infrastructure to strengthen the critical infrastructures by working closely with private sectors and the cybersecurity community

- **Creating a Safer Cyberspace**
  - Creating a safer cyberspace by promoting government, industry, and public involvement

- **Developing a Vibrant Cybersecurity Ecosystem**
  - Developing a vibrant security ecosystem by working with industry and academia to grow the cybersecurity workforce

- **Strengthening International Partnerships**
  - Strengthening international partnerships, especially among the ASEAN members, to address transnational cybersecurity issues

Each of the four pillars envisions the business sector playing a central role. Pillar 3 – a vibrant cybersecurity ecosystem – explicitly describes the government’s efforts to support business.

As other National Cybersecurity strategies, the government invests in R&D. Singapore set up a five-year SGD 130 million (USD 94 million) National Cybersecurity R&D Programme to promote collaboration among agencies, academia, research institutes, and the private sector.\(^{32}\) It is a fraction of SGD 19 billion (USD 14 billion) commitment in the Research Innovation Enterprise 2020 Plan (RIE2020) which seeks to support and translate research into solutions that address national challenges, build up innovation and technology adoption in companies, and drive economic growth through value creation.\(^{33}\) Around 40% of the money will be open for competition. The RIE2020 aims at four primary technology domains, each entailing cybersecurity efforts:

- Advanced Manufacturing and Engineering
- Health and Biomedical Sciences
- Services and Digital Economy
- Urban Solutions and Sustainability\(^ {34}\)

The local market is projected to grow at 9% per year.\(^ {35}\) The global cybersecurity market is expected to grow at a compound annual growth rate of 11.8% from USD 71 billion in 2013 to USD 155 billion in 2020.\(^ {36}\)

CSA started working on initiatives such as the Cyber Security Associates and Technologies (CSAT) programme for training and up-skilling fresh ICT professionals and mid-career professionals for cybersecurity job roles and the introduction of CREST certifications in Singapore. CSA has also signed MOUs with Nanyang Polytechnic (NYP) and the Singapore Institute
of Technology (SIT) to develop cybersecurity talent. Moreover, the Singapore government explicitly declared to ‘build up’ local industry:

_We will build up the industry by attracting and anchoring companies with advanced capabilities. We will also nurture startups to boost the development of niche and advanced solutions and grow local champions to sustain strategic areas of interest. We will also develop market opportunities to bring made-in-Singapore solutions into the global market._

Official declaration from Singapore’s Cybersecurity Strategy

This quote is especially important. Singapore is famous for actively seeking best practices around the globe to tackle their major challenges and exploit opportunities. Singapore’s strategy shows that the policy that Israel and the UK chose years ago – the boost of innovation in cybersecurity business particularly via the government support for – actually worked. Singapore enjoys the presence of all major stakeholders in the city-state: financial services multinationals, Boeing’s first Cyber Analytics Centre outside the US, INTERPOL’s Global Complex for Innovation, NEC’s Public Safety Business, and dozens more. Singapore’s government can afford to procure and effectively utilise any commercially available solution, and it does so indeed. Singapore had been exploiting these advantages to tackle cybersecurity in traditional ways for years. Now it has decided to follow the UK and Israel’s path to boost the local cyber R&D and the local cyber industry. Singapore is the world’s freest economy, providing exceptionally fair and open business environment to all. Nevertheless, Singapore aims for the global market beyond domestic consumption. This strategic approach refutes the ideological arguments, which are often recruited against significant government support for the domestic business sector.

**ESTIMATED GROWTH OF SINGAPORE’S CYBERSECURITY MARKET, 2015–2020**

<table>
<thead>
<tr>
<th>Year</th>
<th>Cybersecurity Services</th>
<th>Cybersecurity Products</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>154</td>
<td>417</td>
<td>561</td>
</tr>
<tr>
<td>2016</td>
<td>163</td>
<td>464</td>
<td>627</td>
</tr>
<tr>
<td>2017</td>
<td>176</td>
<td>511</td>
<td>687</td>
</tr>
<tr>
<td>2018</td>
<td>188</td>
<td>562</td>
<td>750</td>
</tr>
<tr>
<td>2019</td>
<td>201</td>
<td>617</td>
<td>818</td>
</tr>
<tr>
<td>2020</td>
<td>216</td>
<td>673</td>
<td>889</td>
</tr>
</tbody>
</table>

_Compound Annual Growth Rate of 9.3%_
All the three National Cybersecurity Strategies analysed here share strikingly similar approaches when it comes to enhancing administration-business cooperation for the creation and absorption of cybersecurity innovation. The UK, Israel and Singapore have invested significant public funds to incentivise the establishment of academic centres for excellence in cybersecurity at universities to create radical innovation that involves changes in the current practices and processes. Regional concentration of competences is evident in many successful innovations. Israel has created the main IT cluster in Tel Aviv area, and is developing a new cybersecurity cluster in Be’er Sheva. The emergence of the ‘Silicon Roundabout’ in London and the ‘Cyber Valley’ in Malvern bears some resemblance to Israel’s efforts in Be’er Sheva. Similarly, Singapore’s Biopolis for biomedical sciences is among the most ambitious projects the country has ever embarked on.

Direct government support for commercial companies includes:

- providing R&D grants;
- procuring R&D services from commercial companies;
- creating domestic market;
- helping access foreign markets;
- sharing government capabilities with commercial R&D companies.39

Indirect government support for the entire National Innovation System (NIS) includes fiscal incentives and legal frameworks.

- fiscal support and other incentives for non-commercial research institutions and IHLs
- legal and financial support for academia-business cooperation in selected topics (e.g. technology transfer mechanisms)
- tax incentives for R&D expenditure in commercial companies
- infrastructure for co-location.

**FINDINGS:** GOVERNMENTS OF LEADING CYBER POWERS SUPPORT THE BUSINESS SECTOR IN CREATION AND ABSORPTION OF INNOVATION
THIS SHORT ANALYSIS ILLUMINATES THE FOLLOWING FINDINGS:

- Innovation is instrumental for cybersecurity. All three National Cybersecurity Strategies analysed here seek innovation for cybersecurity.
- Successful innovation largely depends on the government strategy and policies. The fact that the world’s leading cyber powers are also leading innovators is not a coincidence.
- Israel and the UK have been dedicating a range of deliberate government policies and resources to support enhanced administration-business cooperation since 2011. These strategies have produced real economic and security value.
- Singapore is currently adopting this approach, including the ‘build-up’ of the local industry.

**SOURCES:**

5. Financial Times, https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb (access: 11/05/2017).
25. NCSC consolidates the expertise of the previously existing: CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related divisions of the Centre for the Protection of National Infrastructure
31. Own elaboration based on the official strategy document.
39. Think U.S. defence mega-contractors and U.S. defence and intelligence agencies
FROM SOURCE CODE TO EXPORT: 
ADVANCED PRIVATE ICT SECTOR AS A CRUCIAL 
PART OF THE NATIONAL CYBERSECURITY 
ECOSYSTEM 
ROBERT SIUDAK

The rising role of the Internet in the economy, Revolution in Military Affairs or the changing patterns of information ecology due to the new media expansion, all these have created a new set of challenges for national strategies in both military and civilian sectors. Cyberspace is a novel area for countries which are struggling to apprehend and secure critical parts of this fast evolving realm – the realm which is gradually becoming the backbone of our information society. In contrast to traditional domains governed and secured by central governments, such as land, sea and air, the unique characteristics of this new field can be found in the building blocks of cyberspace which consists of:

- hardware (physical layer)
- software, protocols (syntactic/logical layer);
- storable and transferable information and ideas (semantic layer).

The novelty of this realm rests on the fact that the first two components are produced by the private entities operating within the open-market paradigm. This simple technical fact must be seen as a rudimentary cause for the far-reaching political consequences, with the most important being that without a large and advanced national ICT sector, a country has severely limited cybersecurity capabilities.

The bigger the better: ICT sector, cybersecurity and innovation

A mature ICT sector should be perceived as the driving force for both national cybersecurity and innovation. It is not a coincidence that a similar set of states is listed in the technology
section of the Fortune 500 Global Rank and Global Cybersecurity Index. The latest 2016 Forbes edition features 33 tech companies. The leading state is the U.S. with 11 representatives, followed by Japan and Taiwan with 5, China with 4, and 3 from South Korea. By comparison, the latest Global Cybersecurity Index & Cyberwellness published by International Telecommunication Union (ITU) and ABI Research in 2015, ranks the U.S. as the most prepared country, with Japan and South Korea coming 5th and China 14th. Poland ranks 11th on the ITU list, with the index 0.592.

The private sector is the main source of ICT solutions in the modern market. The prime cause for it can be traced to the structure of the modern economy. As discussed in the previous chapter, the business sector is
harvesting fundamental and applied research by changing it into experimental development of new products or services. Since the market needs and rules are the catalysts of innovation in the digital economy, it is no surprise that the high-tech section of the Bloomberg Innovation Index from 2015 features the same set of states as the Forbes 500 Global ranking discussed above: the U.S. (1st), China (2nd), Japan (3rd), South Korea (4th), and Canada (5th). \(^5\) 

How all of this influences the security of cyberspace? According to Symantec report, roughly one million new malwares are released every day. \(^6\) Hackmageddon which monitors bigger network attacks counted 1,061 incidents in the last year, which accounts for more than 3 large-scale malicious cyber operations per day. \(^7\) Due to a rapidly changing threat environment, the cybersecurity sector is one of the fastest evolving realms of ICT. Nowhere else innovation is so crucial. To keep up with their adversaries, cybersecurity companies have to be innovative by design. The analysis of the Cybersecurity 500 list which ranks the most innovative cyber companies worldwide confirms that there are two key indicators which allow for the creation of a strong national cyber-innovative ecosystem. \(^8\) The first one is a mature and internationally competitive ICT sector; the second is the existence of the National Innovation System discussed in the previous chapter. The first three countries with the highest number of representatives on the Cybersecurity 500 list in 2017 have them both: the U.S. with 365 firms, Israel with 36 companies, and the UK with 23 representatives.

**CYBERSECURITY 500 RANK – COMPANIES BY COUNTRY**

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>365</td>
</tr>
<tr>
<td>Israel</td>
<td>36</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>23</td>
</tr>
<tr>
<td>Canada</td>
<td>13</td>
</tr>
</tbody>
</table>

Source: Cybersecurity Ventures, *The Cybersecurity 500, 2017*

**Cybersecurity as a comparative advantage**

We are gradually becoming more aware of how vulnerable yet indispensable our networks and systems are. Many reports suggest that 2016 brought about a breakthrough in the public’s perception of cybersecurity. \(^9\) It is no longer a distant and minor problem important only for IT departments. It has become an integral part of our businesses, our financial activities, and our personal lives. We have come to realise that cybersecurity will be one of the fundamental challenges in the coming decades. But this challenge might also be a huge opportunity for those who know how to use it.
Cybersecurity is one of the fastest growing sectors of the ICT market. According to various reports, in 2017 the worldwide spending on cybersecurity products and services is projected to reach more than USD 120 billion.\textsuperscript{10} In the last decade, we were witnessing this market grow by 8–10\% annually, and predictions for 2017–2020 indicate further steady growth with a cumulative sum of USD 1 trillion being spent on cybersecurity in this period. Between 2015 and 2020, the compounded value of products and services securing the Internet of Things (IoT) is estimated to reach up to USD 120 billion – the level of the current overall cybersecurity market value.\textsuperscript{11}

The particularity of this sector lies in the fact that the aforementioned growth is driven primarily by the scale of threats that are rising
exponentially in the cyber domain and to a lesser extent by technological breakthroughs or processes optimisation. It is hard to estimate total losses from cybercrimes for the public and private entities worldwide, but they are estimated to be currently at the level of around 1% of global GDP. Furthermore, researchers predict that by 2021 they will have accounted for more than USD 6 trillion losses annually. We are faced with a rapidly growing market driven by immanently vulnerable nature of the connected technologies.

A strong cybersecurity market might not only become a high revenue niche for national ICT companies, as is the case with Israel and the UK. It should also bring long-term advantages for the country’s overall economy by providing available and affordable cyber products and services for the business and the public sector. This, in turn, helps to increase macroeconomic ratings. Announcements like those by Standard and Poor’s in 2015 about lowering marks for lenders who fail to protect themselves against cyberattacks confirm this dependency. Last but not least, a mature national market providing world-class solution to protect ICT infrastructure should be perceived as a technical base and enabler for any advanced cybersecurity policies and regulations introduced by governments.

Building cyber sovereignty

The benefits that cybersecurity smart specialisation yields to the market are just one side of the equation. The other is the concept of cyber sovereignty. The underlying assumption is that ICT has nationality, which creates important cybersecurity implications. To be able to secure its own cyberspace and to make sovereign policy decisions on the contemporary international arena, a country needs to have a competitive national ICT sector at its disposal. Being able to acquire source codes, develop cutting-edge and dedicated products and services, or cooperate with the producer to monitor the implementation of a bespoke technology under the umbrella of intelligent services is a must in many critical systems. The prime examples of this problem might be China’s ban on Windows 8 operating system over security matters or barring Huawei from pitching for U.S. government contracts because of espionage concerns.

It is important to view the national ICT sector as more than a mere provider of products and services to the market. It is a crucial part of the whole cybersecurity ecosystem based on four main components embedded in the cooperation between the private and the public sector:

It is hard to estimate total losses from cybercrimes for the public and private entities worldwide, but they are estimated to be currently at the level of around 1% of global GDP.
- national cybersecurity human resources with appropriate knowledge and expertise;
- hardware and infrastructure provided by domestic ICT producers and operators;
- available software and logical building blocks (protocols and standards) created, maintained, and serviced by national companies;
- cybersecurity nation-wide system incentivising collaboration between the private and public stakeholders and introducing innovative solutions.

Apart from the already discussed supply side of the domestic ICT market represented by the 2nd and 3rd component and the systemic role reflected in the 4th element, the private sector has to actively participate in educating and training national cybersecurity workforce. The demand for cyber specialists is growing exponentially, with predictions of up to 6 million workplaces and 1.5 million unfilled vacancies globally by 2019. Institutionalised education is lagging behind the fast evolving cybersecurity field, which creates a need for business involvement in order to utilize private sector’s aggregated expertise and experience.

Many national players have already apprehended the strategic role of the domestic ICT sector in their pursuit of secure cyberspace. As presented in the previous chapter, Israel, the UK and Singapore have already introduced dedicated programmes to support national innovation in the cyber domain. Others such as the U.S., China, South Korea, and Japan also actively support their digital industries. The European Union has recognised that in face of the fact that ‘Global cybersecurity and ICT market is dominated by global suppliers from North America’, it has to play a more active role. As detailed in the first chapter of this report, in 2016 the European Commission and the European Cyber Security Organization (ECSO) signed a contractual public-private partnership (cPPP) that aims to develop a competitive European market by triggering EUR 1.8 billion of investment by 2020.

**Poland – untapped potential**

In 2016, the Polish ICT market was worth roughly USD 8.75 billion. It was a result of the steady annual growth of 5-6% on average in the last two decades, with a high 9-10% boost observed in the recent quarters. In 2017 ICT is predicted to account for more than 4.5 % of the total number of employees in Poland and 6 % of Polish GDP. The transformation of the Polish economy in the last 28 years resulted in a huge shift from traditional sectors such as coal mining and shipbuilding into a more service-oriented GDP composition and the rising role of information technologies. The ICT companies which accumulated expertise over that time had a
unique chance to come to the forefront of the digital transformation of the Polish economy. The main asset that has been developed in this process and which could be utilized to build a national cybersecurity ecosystem are human resources. Poland’s abundance of cyber talents has been proven by numerous rankings and hackathons. Polish developers and hackers won almost every well-known cyber contest from Locked Shields (2014) through Capture the Flag cycle (2014) to unofficial developers’ world cup – Hello World Open (2014) and Google Code Jam (2012).

According to HackerRank, Polish developers rank third, just after their Chinese and Russian counterparts. When it comes to Java, Poland tops the list, being followed by other two CEE countries: Bulgaria and Hungary.21 Furthermore, Poland stands second only to Singapore as the world’s leading developer hub from business and investors’ perspective.22 This accelerates the demand for skilled ICT specialist in the domestic market. Current estimates show that 40,000 ICT vacancies are still unfilled, even though Polish universities educate 30,000 new ICT graduates every year.23

Drawing upon the world-class human resources, ICT is one of the most globally competitive sectors of the Polish economy. From startups through medium enterprises to big companies, Poland is a home country for dozens of internationally expanding brands. Many of them are leaders in their market segment, with their R&D departments being a source of unique, cutting-edge technological solutions. Others, due to their innovative business models, are able to compete globally with the biggest players from Silicon Valley or Shenzhen.
But world-class human capital and open business environment are not enough to make cybersecurity ecosystem truly thrive. As postulated in the first chapter of this report, there is a need for a more systemic public-private partnership which can harness available market and government resources to strengthen national cybersecurity. This cross-sectoral cooperation is also a prime requirement for the Polish commercial ICT sector to grow. According to numerous reports, in the last years

Poland’s domestic ICT market has struggled with two main obstacles:

- **Insufficient funding, both external and internal, including high-risk capital.** Enterprises view this factor as ‘the biggest barrier to innovation’.²⁴

- **Reduced demand from the public sector, including central and local governments as well as state-owned enterprises.**²⁵

The former is a particularly problematic issue for cybersecurity and high-tech startups. In order to properly scale up their products and internationalise their offer, they need to have access to high-risk capital to get the project off the ground. In many cases, it is the market itself that forces Polish startups to seek investors abroad among American, French, or British Venture Capital Funds. The gravity of the latter issue rests on the fact that in the last year, public spending in Poland accounted for 42.1% of total GDP.²⁶ This figure shows only central and local government expenditures, excluding publicly owned companies which are occupying first 13 places on the list of the biggest enterprises with Polish capital.²⁷ According to a survey conducted by the Kosciuszko Institute and the Cybersecurity Foundation in May 2017 among Polish cybersecurity companies, 88.9% of enterprises recognised limited demand for innovative products as the main drawback of the domestic cybersecurity market. The strategic importance of both challenges is confirmed by the fact that there are already certain public initiatives in place trying to tackle these problems. The Venture Capital market is slowly emerging in Poland, partly thanks to government programmes like ‘Bridge Alfa’ or ‘Starter’. They combine private and public capital, which allows for the creation of new domestic VC funds. Both programmes are incorporated into a wider agenda of governmental support for the startup sector under the umbrella of the ‘Start in Poland’ brand. New initiatives are also emerging in the state-owned enterprises, many of whom are planning to establish corporate VCs.²⁸ Others such as Witelo, a Fund of Funds designed to reinvest publicly owned assets in Polish startups through international VC funds, has already signed deals with partners like Atomico, Evolution Equity, and DN Capital.²⁹
To tackle scarce public interest in domestic cybersecurity products and services more systemic solutions are needed. Therefore, open collaboration platforms must be established at central and local levels to match the demand with the supply side in order to drive their growth. Once completed, the Cyberpark Enigma project proposed in the governmental Responsible Development Plan might become a core nodal point in the process of fine tuning public needs to the domestic market offer.\(^{30}\) The goal is to attract private Polish-owned companies as well as government-owned entities and academic research centres to cooperate at all levels of the supply chain. Local initiatives such as Cybersec Hub in Krakow, which connects academia, large companies and startups with local authorities and other public partners, might be a workable example of regional cybersecurity ecosystems.\(^{31}\) This, as well as others systemic propositions such as a specially designed startup accelerator have been repeatedly voiced during the Polish Cybersecurity Forum – CYBERSEC PL 2017.

Although, as presented above, some initiatives are already in place, there is a need for key strategic decisions to be made to seize the opportunity provided by the growing cybersecurity market.

To become one of the centres of world-class expertise and products in cyber technologies, at least six initial steps have to be taken:

- Establish nation-wide Public-Private Partnerships on cybersecurity in order to boost investment in the domestic market;
- Set up a range of cybersecurity research and development programmes to attract academics to conduct fundamental and applied research;
- Incentivise entrepreneurs to expand their investments and R&D in the field by introducing special benefit packages for companies partnering within regional or central cybersecurity hubs;
- Attract the public sector to domestic cybersecurity products and make central administration more open to cooperation with enterprises of all sizes: startups, small and medium companies, and national champions;
- Change the legal framework to enable all domestic companies, including startups and SMEs, to take part in the public bids for cybersecurity products and services;
- Prepare and execute a long-term PR strategy to promote Poland as a centre of excellence in cybersecurity.
- Singapore is currently adopting this approach, including the ‘build-up’ of the local industry.
The aforementioned initiatives will enable harvesting technology and human resources and building them into the emerging national cybersecurity ecosystem. Furthermore, smart specialisation in cyber technologies could become a competitive advantage of the entire Polish ICT sector. This, in turn, would support the national economy by changing Poland’s position in the global ICT supply chain. Known for outsourcing simple back- and front-end services, Poland could transform into a centre of innovative and cutting-edge cybersecurity products.

**SOURCES:**


25. PMR, Rynek IT w Polsce 2016..., op.cit.


28. WNP portal gospodarczy, Tauron rozważa utworzenie funduszu typu CVC, 2016, [online] www.energetyka.wnp.pl/tauron-rozwa-utworzenie-funduszu-typu-cvc-275967_1_0_0.html (access: 12/05/2017).


CDR Wiesław Goździewicz (Polish Navy)
Legal Advisor – NATO Joint Force Training Centre (JFTC)
Graduated the Faculty of Law and Administration of the University of Gdańsk in 2002. He then joined the Armed Forces and started his military career as a junior legal officer at 43rd Naval Airbase in Gdynia. He has also served in Public International Law Division of the Legal Department of the Ministry of National Defence. Since October 2009 he has been assigned as the Legal Advisor to the Joint Force Training Centre in Bydgoszcz. Apart from providing legal advice related to the daily functioning of the Centre, his role includes providing training on the practicalities of International Humanitarian Law (IHL) application and legal aspects of military operations, from conventional warfare to space and cyber operations.

Cyprian Gutkowski
Lawyer
Graduated from the Cardinal Stefan Wyszynski University in Warsaw (Faculty of Law and Administration). He also has a degree in Data Security Management from Warsaw School of Economics post-graduate programme. An experienced lawyer, who offers advice on the law, legal procedures and a wide range of associated issues. He is an expert on personal data protection and cybersecurity. He cooperates with Polish Government and non-governmental organizations on the law and information security.

Robert Siudak
Research Fellow, The Kosciuszko Institute
CYBERSEC HUB Manager and Chief Editor of the European Cybersecurity Market Journal. Cybersechub.eu is a platform linking innovative startups from Central and Eastern Europe, global investors, academia as well as local and central authorities in the effort to create regional center of excellence in cybersecurity. Organizer of the startup section at the annual European Cybersecurity Forum CYBERSEC – one of the main public
Lior Tabansky
Cyber Power scholar at Tel Aviv University’s Blavatnik Interdisciplinary Cyber Research Center (ICRC).

Lior offers a uniquely strategic cybersecurity methodology, facilitated by his Political Science & Security Studies expertise (PhD expected in 2017), high-level think-tank, policy and corporate experience, and 15 years of IT-Pro practice. Recently, Lior’s book Cybersecurity in Israel, co-authored with Prof. Isaac Ben-Israel, was published by Springer. Cybersecurity in Israel is the first comprehensive “insider” account of decades of policy evolution, dilemmas and operations. Further, Lior Tabansky develops an original analysis of the roles grand strategy and national innovation system play in cybersecurity.

Asseco Poland is the largest IT company listed on the Warsaw Stock Exchange. It has developed technologically advanced software solutions for companies and institutions of all key sectors of the economy for more than 25 years. Today, Asseco is the number one software house in Central Europe and the sixth largest software vendor in Europe. Asseco Group is present in 54 countries, employing over 22,000 people. It has provided IT technologies to support business operations as well as development at more than 100,000 companies and organizations. While operating in international markets, Asseco has gained extensive experience, combining the know-how of all the Group’s subsidiaries. The synergy of these competencies provides added value to customers who receive the top quality products.
Founded in 2000, the Kosciuszko Institute is a leading, non-governmental and non-profit think tank and research institute. Our mission is to act in the interest of the socio-economic development and security of Poland as a proactive member of the European Union and NATO.

Specializing making strategic recommendations, our Institute lays down the paths for the advancement of key public policies offering substantive support for Polish and European decision-makers alike. Our think tank fellows produce nonpartisan and independent reports and analyses, and their conclusions are an essential source of information for the private sector and civil society.

As a leader among Polish non-governmental organisations, the Kosciuszko Institute runs a range of national and international projects devoted to multifaceted aspects of security, including energy and economic security as well as cybersecurity. Engaging key policy and business stakeholders, the representatives of international organisations and the NGO sector in collaborative efforts, our Institute initiates socio-political debate on the most pressing challenges facing Poland and Europe.

Due to its leadership position, the Kosciuszko Institute attracts the best analysts from all over the world to launch multiple pioneering and innovative ventures. The Kosciuszko Institute is the originator and organiser of the European Cybersecurity Forum – CYBERSEC, an annual conference dedicated to the strategic aspects of cyberspace. The first edition of the event was held in 2015. Recognising its pivotal role as a platform for regular dialogue between key stakeholders, Concise Courses has ranked the event among the top five cybersecurity conferences in Europe. As part of the CYBERSEC initiative, we have also rolled out a national edition of the conference: the Polish Cybersecurity Forum – CYBERSEC PL.