November 2017

THE KOSCIUSZKO INSTITUTE

THE KOSCIUSZKO INSTITUTE POLICY BRIEF

Robert Siudak, Ziemowit Jóźwik

Regional innovation centres and their role in dealing with cyber disruption

authors

Robert Siudak – Research Fellow of the Kosciuszko Institute for innovation and investments in cybersecurity. Chief Editor of the European Cybersecurity Market journal and CYBERSEC HUB Manager. Author of many scientific publications, including two monographs. Doctoral student at the Department of National Security at Jagiellonian University. Studied and conducted research at Tel-Aviv University and Trinity College Dublin.

Ziemowit Jóźwik– Research Fellow of the Kosciuszko Institute for EU cybersecurity law. Deputy Editor of the European Cybersecurity Market journal and International projects coordinator. Graduated in law and Ukrainian studies. Completed a post-doctoral course in specialist translation from Ukrainian. Coordinated projects related to border security and the situation in Ukraine. Co-editor of *Addressing Security Risks at the Ukrainian Border Through Best Practices on Good Governance* (NATO SPS Series).

Regional innovation centres for cybersecurity

In collaboration with Global EPIC:
Anat Karmona, CyberSpark (Israel)
David Crozier, Centre for Secure Information Technologies – CSIT (United Kingdom)
Dan Craigen, Global Cybersecurity Resource (Canada)
Darin Andersen, CyberTECH Network (United States)
Richard Franken, The Hague Security Delta (Netherlands)

The leading competence and innovation centres for cybersecurity are established all around the world in the form of regional hubs. Building local ecosystems allows for real and efficient cooperation between the triple helix of government (both regional and national), university centres for research and innovation, large international companies, local SMEs and startups. Additional support from the venture capital community is also a feature of these ecosystems. The synergy that develops within such structures enables the accumulation and flow of knowledge, good practices and key competences. Education and training of world-class specialists and innovators through both university courses and participation in the private sector, fosters the development of medium – and long-term research projects, as well as investments in promising technologies at the early stages of their development. In turn, an innovative sector of products and services can develop on this foundation of basic and applied tasks. Below is a list of selected innovation centres for cybersecurity.

ISSN 1689-9873

CyberSpark (Israel)

Israel, due to its turbulent history, geographic location and unstable political situation in the region, maintains an extensive army, including cybernetic units. These units are the birthplace of human resources and a base for specialists in the commercial sector of products and services that secure ICT infrastructure. Israel's choice of intelligent specialisation in cybersecurity has translated into notable financial effects for the entire economy. In 2015, this industry generated an income of 3.75 billion dollars, which constituted more that 1% of GDP.[1] Currently, 365 companies in the cybersecurity sector operate in Israel, 65 of which were established in 2016 alone.[2] In the same year, Israeli startups dealing with the security of ICT collected a total of USD 581 billion in investments, placing second in the world in this respect, right after American companies.[3]

In 2014, in collaboration with the Israeli National Cyber Bureau, governmental administration, Beer-Sheva authorities, Ben-Gurion University and the global tycoons of the industry (e.g. Oracle, IBM and Lockheed Martin) CyberSpark was launched. It is an Israeli space for innovation in cybersecurity that supports research in and development of commercial products and services. Furthermore, as part of its flagship initiatives, CyberSpark provides:

1) Research centre: co-created with the Ben-Gurion University;
2) R&D hub: a development zone for commercial products supported by tax exemption and public grants;
3) Training centre: offering training in cybersecurity;
4) Innovation hub: a networking platform;
5) Incubator: supporting the development of new cyber projects;
6) Analytical centre: in close cooperation with IL-CERT.

Governmental administration supports CyberSpark not only through infrastructure, but also through economic incentives, such as reduced income tax for R&D or refunding even up to 30% of the gross remuneration of experts who work on a technology that is particularly valued on the market. Furthermore, the national Computer Emergency Response Team (CERT) was deployed along with military intelligence and technological units operating in the cyber sector as part of the new regional cybersecurity ecosystem in Beer-Sheva.

Centre for Secure Information Technologies (United Kingdom)

The British sector of security pro ducts and services for ICT constitutes the largest national cybersecurity market in the European Union. In 2015, its estimated value was 4.8 billion Euro, which corresponded to 20% of the entire EU market.[4] Furthermore, Great Britain has developed one of the world's largest cybersecurity sectors, which currently employs approximately 40,000 people within

1 Israel's National Cyber Bureau data. (8) HM Government, *The UK Cyber Security Strategy 2011-2016: annual report*, 14 April 2016, https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report [26 October 2017].

2 YL Ventures Ltd. data; https://techcrunch.com/2017/01/23/trends-in-israels-cybersecurity-investments/ [27 October 2017].

3 Start-Up Nation Central Ltd. data; www.startupnationcentral.org [27 October 2017].

4 NIS Platform, *Business Cases and Innovation Paths, NIS Platform Working Group 3 (WG3), Final, Version 1.1*; https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents, p. 24–25 [26 October 2017].

firms developing or providing cyber security products and services and upwards of 100,000 if CISO functions and the broader services are included.[5]

This commercial success is supported by an extensive network of research centres for cybersecurity that associates 14 Academic Centres of Excellence in Cyber Security Research (ACE-CSR) throughout Great Britain and Northern Ireland. The title of an ACE-CSR is given to universities that conduct innovative research on cybersecurity and educate world-class post-doctoral specialists in this field. Moreover, another important support initiative for the development of new technologies, including ICT security solutions, is UK nationwide network of innovation centres, which associates seven academic centres (called Innovation and Knowledge Centres – IKCs).
Queen's University in Belfast, which is listed as both a research centre for cybersecurity and an IKC, established the Centre for Secure Information Technologies (CSIT) in 2009. The aim of the centre is to create an innovation hub for cybersecurity by building a comprehensive ecosystem of local and global stakeholders. This is why the CSIT actively supports the development of the Belfast Cyber Security Cluster, which associates more than 40 companies hiring 1200 employees. Furthermore, the centre, as part of its activity, has already attracted many foreign direct investments in the sector of high technologies, and the partners of the CSIT currently include global corporations, such as Allstate, BAE Systems, Thales, Infosys, Equiniti and Direct Line Group. The CSIT also provides education for university students through its MSc Applied Cyber Security and carries out internal R&D in fields such as:

- Security of critical infrastructure;
- Device authentication;
- Malware targeting mobile devices;
- Post-quantum cryptography.

5 HM Government, *The UK Cyber Security Strategy 2011-2016: annual report*, 14 April 2016, https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report [26 October 2017].

Global Cybersecurity Resource (Canada)

Canada is the fourth largest innovation hub for cybersecurity in the world, considering the amount of venture capital investment in this sector between 2012 and 2016 (right after the US, Israel and Great Britain).[6] In particular, a unique ecosystem has developed in Ottawa (the capital of Canada), in which an active community of more than 90 cybersecurity startups and SMEs from the cybersecurity sector was able to obtain funding amounting to over 250 million dollars from VC investors between 2011 and 2015.

Using this potential, Carleton University launched a business accelerator in 2016, called the Global Cybersecurity Resource (GCR; cugcr.ca). It is located in Ottawa's largest innovation hub (Bayview Yards) and receives funding from FedDev Ontario's Investing in Regional Diversification Initiative. The GCR builds upon two key programs from Carleton: the Technology Innovation Management Program (TIM; timprogram.ca) and Lead to Win (LTW; leadtowin.ca). As such, key business objectives (e.g., growth, scaling and globalization of young companies) draw from the competencies and knowledge developed both from the market and within universities (e.g., applied theories, focused projects). Services provided by the GCR to cybersecurity companies include:

- Access to the international network of business contacts through the Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity (Global EPIC; globalepic.org);

- Building upon the LTW programme, which aims to lead a company from the concept stage,

6 Deloitte, *Harnessing the cybersecurity opportunity for growth Cybersecurity innovation and the financial services industry in Ontario*, October 2016; http://www.oce-ontario.org/docs/default-source/default-document-library/oce-tfsa_cyber-brochure-exec-summary-online-oct19.pdf?sfvrsn=4 [26 October 2017].

through incubation and acceleration, to growth and scaling up. The stated objective is that a new company should aim for revenues of at least C$1 million within three years. The programme is considered to be one of ten best university incubators in North America;[7]

- Provision of security management services for small companies. The first offering is an open-source based attack alert system supported by a Security Operations Centre;

- Access to "Pathways," a new pedagogical approach to measurably enhance the knowledge and skillsets of students. The initial set of Pathways focus on important areas of entrepreneurism and cybersecurity.

The GCR follows the principle "localise the global and globalise the local" or "co-create globally and benefit locally." Thus, the centre conducts programmes that are aimed to 'localise' global initiatives (e.g., joint projects, standardization) and resources (e.g., international expertise, mentoring, investment), while globalising (e.g., small local companies accessing global markets and expertise).

CyberTECH (United States)

Despite often divergent estimates concerning the value of the global market of services and products for cybersecurity, the US, regardless of the applied research methodology, remains its leader, with the share of about 20%. The US hegemony in the industry is clearly proven by the Cybersecurity 500 list, which presents 500 top innovative companies from the cyber sector, and includes 365 American companies (Israel places second with 36 companies).[8]

The potential of the Silicon Valley and other innovation centres in California motivated the launch of the California Cybersecurity Task Force (CCTF) in 2013, operating as a public-private partnership, with support from the governmental administration and a community of entrepreneurs. In 2015, the Cyber California coalition was formed as the project of the CyberTECH network. The purpose of the network is to promote the western state as a 'global epicentre of commercial cybersecurity'. Particular emphasis in the cooperation between stakeholders has been put on technological challenges and business opportunities related to the rapid development of the Internet of Things (IoT) and Smart & Safe Cities – the intersection of Smart Cities and Cybersecurity. Many initiatives operate under the umbrella of the CyberTECH brand:

- Specialised centres of education in cybersecurity (Centres of Cybersecurity Excellence in Education) established at universities and state colleges;

- The cybersecurity ecosystem created as part of the San Diego Cyber Center for Excellence, established in collaboration with local authorities, California State University, University of Phoenix and companies interested in investments in the cyber sector in the San Diego region (e.g. Cyber Flow Analytics, ESET, as well as Ernst & Young, etc.). The hub comprises over 100 companies hiring 7620 employees. The region is unique in that the army and its contractors have a significant share in the cybersecurity sector (even up to 50% of employed persons);

- The enterprise development network, which offers business services and support for young companies through the NEST coworking space and a six-month resident entrepreneur programme.

- US Ignite Smart Gigabyte communities project run with partnership with US National Institutes of Science. It Accelerates the development of advanced gigabit applications that cannot run on current networks as the bedrock of smart communities by identifying new economic and social opportunities created by those applications.

7 Sprott Scholl of Business, *Carleton's Lead To Win program for entrepreneurs named one of top ten in North America*, 4 November 2015, https://sprott.carleton.ca/2015/carletons-lead-to-win-program-for-entrepreneurs-named-one-of-top-ten-in-north-america/ [28 October 2017].

8 Cybersecurity Ventures, *The Cybersecurity 500*, 2017, Q1; https://cybersecurityventures.com/cybersecurity-500/ [24 October 2017].

- Smart & Safe Cities Institute developed by CyberTECH, focusing on the state of smart & safe cities, best practices, the cultural aspects of creating safe cities, including elements of Smart Cities and IoT that make people nervous about connecting wearables, "liveables" and "driveables" to the Internet to form smart cities.

The Hague Security Delta (Netherlands)

The value of the cybersecurity market in the Netherlands is estimated at between 0.4 and as much as 7.5 billion Euro a year, depending on the applied methodology.[9] Regardless of what indicators are used, this places the Netherlands among the leaders of this sector in Europe. Moreover, the Netherlands public administration carries out a particularly active foreign policy of multilateral cooperation in cybersecurity. The Global Commission on the Stability of Cyberspace, which began operating in 2017, supports the implementation of coherent standards for security and stability in the cyberspace, while the Global Forum on Cyber Expertise, operating since 2015, aims to increase the cyberspace capability of the stakeholders of the agreement. The tools used for this purpose include not only good practices and political strategies, but also selected technical and procedural standards. The Netherlands is the key initiator of the development of both platforms.

The most important security cluster in the Netherlands is The Hague Security Delta (HSD). This Dutch cluster is active in the field of cyber security, national & urban security, critical infrastructures and forensics It currently associates more than 260 partners, including businesses (corporates, SMEs & start-ups), governments and knowledge institutions. HSD aims to stimulate cooperation and sharing knowledge, contributing to innovative security solutions, more business activity and a more secure world. Therefore HSD provides access to market, knowledge, innovation, talent and capital. Its most important initiatives include:

- SME Connect point: provides small and medium-sized enterprises from the security sector with information on opportunities concerning grants, business partnerships and latest research, and initiates dedicated networking actions;

- Security Startup Accelerator: launched in collaboration with the World Startup Factory, its aim is to provide business support for the development of young companies from the security sector that want to scale their offer quickly. Participants of several-month-long programmes are provided with mentoring, access to expert knowledge, a network of contacts, a number of free business services, etc.;

- City Deal Urban Security: a programme that enabled the launch of 11 living labs in partner cities. It aims to address urban security challenges and, at the same time, present them as a chance for development for the sector of security services and products;

- National Cyber Testbed:[10] a programme of realising the building of a national platform for testing cybersecurity solutions within the existing public and private infrastructure. The programme focuses on solutions designed for the Internet of Things (IoT) and critical infrastructure. Its aim is not only to ensure a sufficient level of security, but also to develop innovative

9 Hendriks A., Brandt D., Turk K. (VKA) and Kocsis V., Daan In't Veld, Smits T. (SEO Economisch Onderzoek), *Economische Kansen Nederlandse Cybersecurity-Sector: Een verkenning*, 17 May 2016; https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansenned-erlandse-cybersecurity-sector.pdf [20 October 2016]. Compare: The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity. Putting it in perspective*, December 2016 https://www.thehaguesecuritydelta.com/media/com_hsd/report/123/document/HCSS-Dutch-Investments-in-ICT.pdf [20 October 2016].

10 The Hague Security Delta, *Verkenning van Nut, Noodzaak en Haalbaarheid van een Nationaal Cybertestbed*, 2016; https://www.thehaguesecuritydelta.com/media/com_hsd/report/115/document/NNH-NCT-DEF-Site.pdf [26 October 2017].

products and services based on trial implementations enabled by the platform;

- At the Cyber Security Academy, scholars and lecturers together with experts from private and public sectors translate cyber security related issues into a varied range of multidisciplinary learning tracks for highly educated professionals. The CSA's core is a scientific master's programme in Cyber Security. The CSA also initiates and stimulates the development and supervises the implementation of other innovative Master's degree programmes, several shorter courses, masterclasses and tailored tracks in the field of cyber security.

- HSD Campus: houses both the Innovation Centre, which leads R&D and project incubation, and the International Centre, which supports the internationalisation of the regional market.

Furthermore, HSD was one of the main organisers of the International Cyber Security Week, which took place on 25–29th September 2017 in the Hague. It comprised 80 events attended by 4300 participants from 70 countries, including the representatives of public administration, business, universities and the third sector.

International cooperation between regional cybersecurity ecosystems

As presented above, across the globe, ecosystems that bring together the academia, industry and government respond to cybersecurity threats and provide opportunities for economic development. These centers of excellence have developed mostly independently, driven by local and national objectives. The leaders of these keystones have become aware that the challenges of cybersecurity require global paradigm-shifting platforms and cooperation that reflect regional and local imperatives. Underpinning this perspective is a conscious attempt to '*glocalise*', or localise the global and globalise the local.

To tackle these challenges, on 10 October 2017, the inaugural meeting of the Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity (Global EPIC) took place during the 3rd European Cybersecurity Forum – CYBERSEC 2017 in Krakow, Poland. This initiative will see 13 global ecosystems co-creating and adopting world-changing solutions to high-impact cybersecurity challenges, both current and emergent. Combining their knowledge, experience and expertise, they will develop innovative solutions, drive knowledge sharing, perform trend analyses and research, and exert influence and set standards on a global level. The ecosystems involved come from 10 different countries spanning three continents, reflecting the truly global nature of the platform. Global EPIC will focus its efforts on 10 value-generating initiatives, co-creating globally and benefitting locally:

1) **Network:** each ecosystem provides resources and processes. These offers include: (i) Soft landing services, (ii) Connectivity with expert advisors, (iii) Shared operational tools and facilities, (iv) Ecosystem-specific information, and (v) Sharing knowledge and experience;

2) **Projects**: enable community-generated solutions to domain specific challenges (e.g., internet of things, health systems and financial systems);

3) **Talent:** create development programs to enhance skillsets and knowledge of individuals.

4) **Exchange:** enable matchmaking between otherwise disparate ecosystem entities, e.g. connecting an enterprise in one ecosystem with a specific mentor in another ecosystem;

5) **Evaluation:** contribute to a structured discussion on how to evaluate the resilience of system-of-systems against cyber-attacks;

6) **Content:** enable content sharing across ecosystem organizations. Examples of such content would be datasets, localized social networking feeds and journal articles;

7) **Emerging:** enable horizon scanning, anticipation of emerging issues, trend analysis and investigate theories of new domains;

8) **Advocacy:** use its globally reach and status to advocate for, and raise awareness of, causes, policies, and recommendations;

9) **Investment:** strive to become an engine behind a global framework programme for research and innovation and play a major role in defining budget allocation and prioritization;

10) **Standards:** act in a synchronizing role to standardize our understanding of Cybersecurity.

The 13 ecosystems are: CyberSpark (Israel), Centre for Secure Information Technologies (UK), The Hague Security Delta (Netherlands), Global Cybersecurity Resource – Carleton University (Canada), University of New Brunswick (Canada), CyberTech Network (US), The Kosciuszko Institute (Poland), Politecnico di Torino (Italy), La Fundación INCYDE (Spain), Cyber Wales (UK), bwtech@UMBC (US), Procomer (Costa Rica), Innovation Boulevard Surrey (Canada).

GLOBAL EPIC
Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity

Digital innovation Hubs in Poland

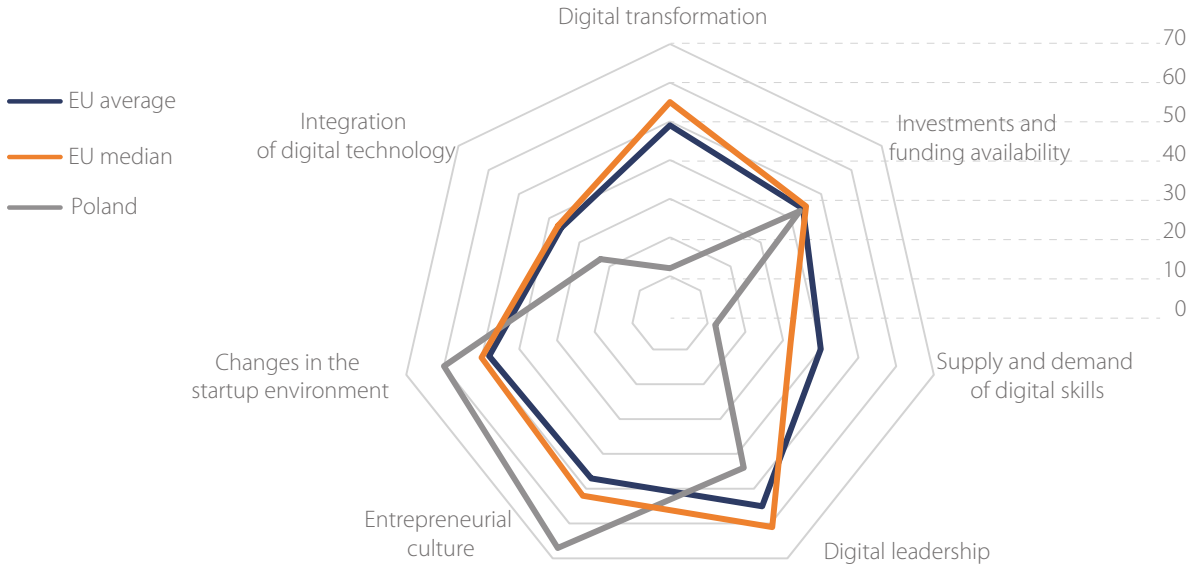
According to a survey by the European Commission (EC), Poland is one of the EU member states with the least beneficial conditions for the digitisation of the economy in terms of investments and access to finance, digital infrastructure, e-leadership, supply and demand of digital skills as well as entrepreneurial culture. Along with Bulgaria, Croatia, Greece, Latvia, Romania and Hungary, Poland ranks among countries that are the least adapted to the fourth industrial revolution.[1] Even though Poland boasts a significant potential with respect to entrepreneurial culture and the evolution of the ICT startup environment (exceeding the EU average by 20 points and 12 points, respectively[2]), it falls behind with respect to digital infrastructure (e.g. access of companies to broadband Internet or the use of CRM and ERP systems), supply and demand of digital skills (patent applications, percentage of total persons employed that have ICT specialist skills and percentage of total persons employed provided with mobile devices by their employers) and integration of digital technologies (enterprises selling at least 1% of turnover online, total turnover from e-commerce, enterprises that did electronic sales to other EU countries, sending of e-invoices suitable for automatic processing, use of cloud computing services of medium-high sophistication, use of RFID technology and percentage of companies that use that use two or more types of social media). Poland has scored from 13 to 30 points below the EU average in each of these categories.[3] Overall, Poland is the 23rd of 28 member states that have been classified for support for the digital transformation of the economy.

Likewise, Poland has placed 23rd in the EC's *European Innovation Scoreboard 2016*, ahead of only Bulgaria, Croatia, Romania, Latvia and Lithuania, which marked the country as one of the 'moderate innovators'.[4] Notably, Poland's annual improvement in innovation indicators is slow, amounting to 0.1% and placing the country 22nd in the EU. This is especially disadvantageous considering that some of Poland's neighbours in the ranking achieve much better results (e.g., Latvia, 4.0%; Lithuania, 2.4%; Bulgaria, 1.4%).[5] Among the indicators that position Poland well below the EU average, the following are worth mentioning here: low cooperation between innovative small and medium-sized enterprises (SMEs), few companies that have implemented innovation within a given entity and the number of product, processual, organisational and marketing innovations in SMEs. Poland has also scored low in terms of financing of R&D (in both public and private sectors) and venture capital.[6] This trend is clearly visible in the data collected by the Central Statistical Office

1 European Commission, *Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses*, January 2017, pp. 4, 47.
2 *Id.*, p. 103.
3 *Id.*, p. 47.
4 European Commission, *European Innovation Scoreboard 2016*, s.12.
5 *Id.*, p. 15.
6 *Id.*, pp. 67 and 86–89.

Figure 1 Poland as a EU Member State

Digital Transformation Scoreboard 2017. Source: compiled based on European Commission, *Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses*, January 2017.



in Poland (CSOP), according to which expenditure on innovation fell in 2016 by 9% among industrial companies and by 15.3% among service companies, compared to 2015.[7]

In the Global Innovation Index for 2016, Poland ranked 39th, falling behind most EU member states. However, since this was a gain of 7 ranks compared to 2015, the result may reflect a positive developmental trend.[8] Polish economy and export are based on high-tech products only to a small degree; the share of high-tech in export amounted to 8.5% in 2015. Growth rate and a low balance are also unsatisfactory, which indicates that Poland remains to a large extent impotent on the market of advanced technology, absorbing goods manufactured abroad.[9]

The mid-period Digital Single Market Strategy review leads to similar conclusions regarding the systemic insufficiencies in Polish economy. One of the key points presented in the document is the need to limit the disproportions between the most technologically innovative and advanced regions of the EU and areas that fail to appropriately stimulate innovation and digital transformation with EU funding.[10] Likewise, the evaluation of the implementation of the programme for research, technological development and innovation, financed as part of the Seventh Framework Programme for Research, Technological Development and Demonstration (FP7) and the Competitiveness and Innovation Framework Programme (CIP) between 2007 and 2013, underlines the insufficient contribution of the countries of Central and Eastern Europe. Furthermore, the activity of entities from this part of EU was found to be lower than expected.[11] The aforementioned evaluation

7 *Działalność innowacyjna przedsiębiorstw w Polsce w latach 2014-2016*, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/nauka-i-technika/dzialalnosc-innowacyjna-przedsiebiorstw-w-polsce-w-latach-2014-2016,14,4.html [30 October 2017].

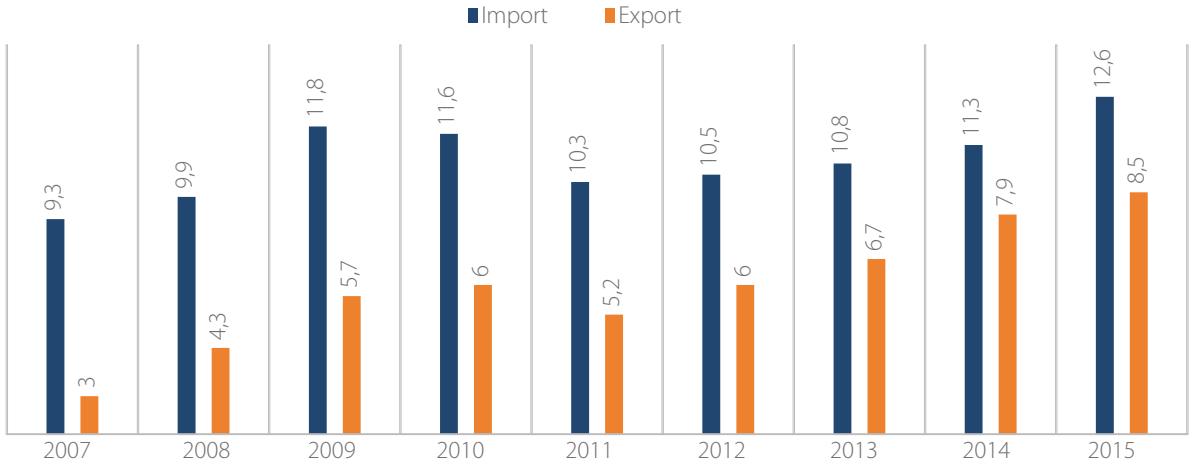
8 *The Global Innovation Index 2016. Winning with global innovation*, https://www.globalinnovationindex.org/ [30 October 2017].

9 CSOP, *Science and Technology in 2010, Warsaw 2012;CSOP, Science and Technology in 2015*, Warsaw 2016.

10 Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead http://europa.eu/rapid/press-release_IP-17-1232_pl.htm [20 June 2017].

11 Commission Staff Working Document, *An assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007–2013)*. Accompanying the document: *Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*, C(2016) 4400 final, SWD(2016) 215 final, SWD(2016) 216 final, SWD(2016) 210 final, 2016, p. 29.

Table 1 Import and Export of High-Tech Products in Total Polish Import and Export [%]
Source: compiled based on European Commission, *Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses*, January 2017.



also underlined that despite an overall improvement in R&D coordination within the EU, the results may not be fully reliable due to the insufficient contribution from Eastern European countries.[12] Poland took part in a total of only five projects within the FP7; for comparison, Germany took part in 99 projects, Spain in 60, and Italy in 82.[13] However, bear in mind that no Polish company and only three companies from Central and Eastern Europe (from Estonia, Hungary and Slovenia) took part in R&D projects as part of FP7.[14] To summarise, the data provided in the evaluation of EU financing for cybersecurity R&D and innovation between 2007 and 2013 show a strong dominance of Western European countries (in Germany alone there have been implemented three times as many project as in the whole Central and Eastern Europe).[15] According to the European Cyber Security Organisation (ECSO; EC's partner for public-private partnership on cybersecurity),[16] the main barriers for SMEs in Central and Eastern Europe in terms of access to pro-innovation EU funding include lower language competences and poorly coordinated and overly bureaucratic distribution of funds at the level of management institutions. Another important issue diagnosed in ECSO analyses is the lack of competences among the local SMEs for participating in long-term building of consortia, which are indispensable in order to carry out projects supported by EU funding. The primary reasons for this state of affairs include insufficient funds (i.e. unwillingness or inability to invest in R&D). Another challenge is insufficient knowledge about the opportunities offered by EU support programmes and difficulties with applying for them.

Digital Innovation Hubs

Establishing Digital Innovation Hubs as network structures that allow for cooperation and accumulation of the stakeholders' potential for stimulating R&D is an opportunity to limit the aforementioned negative developments.

Support for Digital Innovation Hubs constitutes a key part of the EU's strategy for Digitising European Industry. According to EC's data, digitising products

12 Commission Staff Working Document, *An assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007–2013)*. Accompanying the document: *Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*, C(2016) 4400 final, SWD(2016) 215 final, SWD(2016) 216 final, SWD(2016) 210 final, 2016, p. 26.

13 *Id.*, p. 33.

14 *Id.*, p. 32.

15 32 in total, compared to 99 in Germany (3 in Bulgaria, 7 in the Czech Republic, 5 in Estonia, 4 in Hungary, 5 in Poland, 8 in Romania and 2 in Slovenia).

16 Position Paper WG4, *Support to SME's, coordination with countries (in particular: East EU) and regions. Draft document with initial description of priorities and activities*, p. 6.

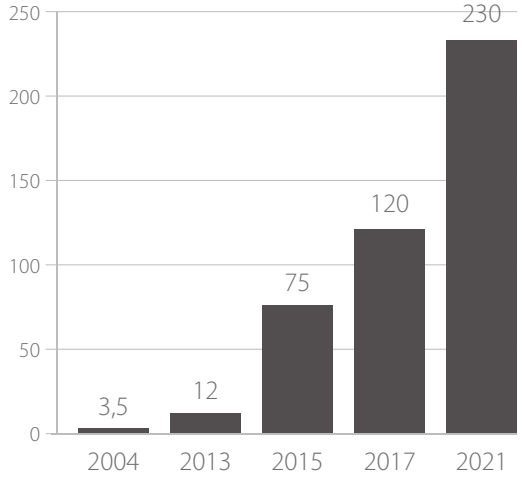
and services will increase the annual industrial revenue in the EU by over 110 billion Euro over five years,[17] which is why it is so important to develop means of dynamising this process. The European network of Digital Innovation Hubs, which aims to provide European industry with advanced digital competences and technology, is planned to drive Economy 4.0 in Europe.[18] EU's primary actions for the development of Digital Innovation Hubs comprise:

- Mobilisation of regional and structural funds in order to build regional and national reference centres as part of digital innovation development in selected EU regions;
- Allocation of EUR 500 million for the construction of a European network of Digital Innovation Hubs as part of the Horizon 2020 Programme in order to cooperate with innovative ecosystems on major development challenges;
- Mobilisation of EC's funding for the establishment of international networks, integration of distributed activities into a single support system for interregional innovative ecosystems, allocation of special funding as part of framework financing programmes, and the establishment of Digital Innovation Hubs in less-developed regions of the EU.

In addition, the EC plans to support the development of Digital Innovation Hubs in countries that joined the EU after 2004[19] in order to eliminate the disproportions between each region and respond to the diagnosed issues related to innovation and the digitisation of the economy. Thus, by following the main directions of the EU's pro-innovation policy, Poland could become the regional leader in this respect and aggregate the innovative potential of Central and Eastern Europe by creating favourable conditions for businesses dealing with new technologies for enterprises within the Three Seas Initiative.

Considering the dynamic development of the global cybersecurity market, which is expected to reach USD 230 billion in 2021, EU's growing interest in the development of industrial and technological resources in the area and the compatibility with national security interests and possible stimuli for economic innovation, cybersecurity is one of the most interesting aspects that can be developed by Digital Innovation Hubs.[20]

Figure 2 Value of the Global Cybersecurity Market (in bln USD)
Source: Siudak R., *From source code to export: advanced private ICT sector as a crucial part of the national cybersecurity ecosystem* [in] *Security Through Innovation. Cybersecurity Sector as a Driving Force in the National Economic Development*, The Kosciuszko Institute, 2017.



17 European Commission, *Digital Single Market – Digitising European Industry Questions & Answers*, Brussels, 10 May 2016, http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm [30 October 2017].

18 European Commission, *Digitalising European Industry*, https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry [30 October 2017].

19 European Commission, *Call for Digital Innovation Hubs in EU13 Member States*, https://ec.europa.eu/digital-single-market/en/news/call-digital-innovation-hubs-eu13-member-states [30 October 2017].

20 Siudak R., *From source code to export: advanced private ICT sector as a crucial part of the national cybersecurity ecosystem[in] Security Through Innovation. Cybersecurity Sector as a Driving Force in the National Economic Development*, The Kosciuszko Institute, 2017, p. 48. Compilation based on: Gartner, *Forecast Analysis: Information Security, Worldwide, 1Q16 Update, 2016; Visiongain, Cyber Security Market Report 2016-2021, 2016; Cybersecurity Ventures, Cybersecurity Market Report Q1 2017, 2017; Markets and Markets, Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region – Global Forecast to 2021*, 2016.

Throughout the world, national competences and technological resources in the field of cybersecurity are strengthened through innovation hubs that emerge within the regional ecosystems and enable cooperation between university R&D centres, local SMEs and startups and large international companies (both multinational corporations and national leaders). Synergies are created within such network structures that allow for the accumulation and flow of knowledge, good practices and key competences. Below are framework recommendations for the establishment of these cooperation platforms that have been delivered during the 3rd European Cybersecurity Forum – CYBERSEC 2017.

Regional ecosystems

In the context of the development of technological and industrial cybersecurity resources through Digital Innovation Hubs, it is worth emphasising the role of individual regions in stimulating innovative economy. It is in the regions where the primary 'strategic resource' concentrates, that is, the knowledge resulting from direct interactions within the ecosystem comprising organisational culture, infrastructure, a skilful pro-innovation policy on the part of the local public administration and the R&D potential of scientific centres.[21] Furthermore, according to the Polish Supreme Audit Office's (SAO) report 'Implementation of Innovation by Universities and Technology Parks', some technology parks were unable to effectively carry out their tasks of creating conditions for the development of technology and innovation companies, for the development of innovative enterprises, and of assisting newly-established companies in the early stages of their operation due to their location in regions with insufficient innovative potential and weaker development.[22] Consequently, entities that are able to take advantage of a regional strategic resource have the best chances for success in supporting the development of innovative solutions in specialised areas of technology, such as cybersecurity. The relationship between regional conditions and the success of Digital Innovation Hubs in cybersecurity can be clearly seen in the examples presented in this paper, as they show the specific links between the local leading academic centres, the private sector and public administration (e.g., the Israeli CyberSpark). Notably, this fact has been acknowledged in the Cyberpark Enigma Programme within the Strategy for Responsible Development and the National Cybersecurity Policy Framework of Poland for 2017–2022, which is based on the leading Polish research centres (Warsaw, Krakow, Wroclaw, Poznan and the Tricity), and the establishment of a Scientific Cybersecurity Cluster.

R&D centres and the expansion of educational and training offers

Due to the constantly growing employment gap in cybersecurity and the need for innovative solutions that would keep up with the dynamic development of threats, a Digital Innovation Hub also constitutes the centre of cybersecurity expertise. A Digital Innovation Hub should cooperate closely with the leading academic centres to allow the educational offer to expand and to facilitate R&D followed by the implementation and commercialisation of R&D results. A Digital Innovation Hub also enables a continuous exchange of knowledge and experience between business and the academia. This, in turn, provides the private sector with constant access to innovation and R&D results, while allowing the scientific community to implement and apply its solutions and access knowledge related to business activity and market functioning, and enabling the expansion of the scientific staff with specialists employed in companies. An example of such a mode of operation is the cooperation between CyberSpark and Ben-Gurion University in Beersheba or between the Canadian Global Cybersecurity Resource and Carleton University. The CYBERSEC HUB in Krakow, described below, cooperates with both the Krakow University of Technology and the AGH University of Technology, being a partner of the former's developing Cybersecurity Centre.

Information exchange platform

An important aspect of a Digital Innovation Hub, especially in Central and Eastern European countries, is the establishment of an information exchange

21 Gust-Bardon N., *Innowacyjność w aspekcie regionalnym*, https://www.ur.edu.pl/file/15836/05.pdf [30 October 2017].

22 Najwyższa Izba Kontroli, *Wdrażanie innowacji przez szkoły wyższe i parki technologiczne*, Warsaw 2013.

platform that will gather up-to-date data about the forms of public support for companies, investments and potential business partners. Such a platform will facilitate mapping the stakeholders of the cybersecurity sector, building consortia, applying for public funding, carrying out joint projects, enterprises and marketing activities and accessing market analyses and assessments of demand for particular solutions. The aforementioned ECSO analyses also indicate the share of Central and Eastern European entities in EU pro-innovation support programmes for cybersecurity could be increased immediately by creating a platform for the exchange of information on current cyber-threats and by either allocating direct funding for the implementation of projects aimed at improving the cyber-resistance of SMEs[23] or by establishing special, easy-to-acquire, small grants for the construction of the basic cybersecurity infrastructure among SMEs.[24] Other proposed solutions include collecting good practices, based on the experience of Western European companies in carrying out EU projects,[25] that would be well-adjusted to regional conditions. Information on the form of EU support could also be shared through social media, digital platforms and business networking platforms.[26] Digital Innovation Hubs should publish knowledge on EU support opportunities for R&D in local SMEs and offer support in establishing consortia and applying for EU funding, thus ensuring stable financial, infrastructural and experimental foundations that would help to test implementations and acting as intermediaries in contacts with the management institutions and the public administration (local, national and European). This is especially important for companies from Central and Eastern Europe, as they do not possess the appropriate resources and competences to constantly monitor the EU decision-making process and take part in it (in contrast to companies from Western Europe, which have developed strategies for government affairs, lobbying activities and building relationships with the most important European stakeholders in the cybersecurity sector).

Incubators and accelerators of innovative startups

We are witnessing unprecedented dynamic evolution of cyber-threats that enforce a constant updating and expansion of solutions in IT security. Effective protection against cyber-threats requires 'radical innovation'.[27] Such dynamics promotes innovative (and frequently niche) offer of startups which are able to keep up with the quickly changing landscape of threats related to, among others, the Internet of Things (IoT), security of unmanned aerial vehicles, management of vulnerabilities and risk,[28] blockchain technology and Artificial Intelligence. The appearance of as many as three startups in the top ten of the 500 Cybersecurity list of 2017, along with global technology leaders, is a testament to the role of startups on the cybersecurity market. Furthermore, some of the other top companies in the list owe their success to taking over or acquiring the innovative solutions that were developed by startups. A model of development that is based on high-risk operating conditions and aims to provide a considerable, quick scalability of the offer makes it possible to achieve a highly dynamic growth in the entire sector, but requires systemic support for startups. To this end, Digital Innovation Hubs should launch incubation and acceleration programmes to foster the development of innovative solutions during the seed and pre-seed phases, which are the key, and frequently the most difficult, stages of development in startups. The acceleration programmes offered by Digital Innovation Hubs should include:

- Financial support;
- Infrastructural support (offices, bureaucracy handling, promotion and marketing);

23 Position Paper WG4, *Support to SME's, coordination with countries (in particular: East EU) and regions. Draft document with initial description of priorities and activities*, p. 7.

24 Position Paper WG4, *Support to SME's, coordination with countries (in particular: East EU) and regions. Preparatory notes*, p. 5.

25 Position Paper WG4, *Support to SME's, coordination with countries (in particular East EU) and regions. Draft document with initial description of priorities and activities*, p. 7.

26 Position Paper WG4, *Support SME, coordination with countries (in particular East EU) and regions. Preparatory notes*., p. 5.

27 Tabansky L., *Innovation Made Possible: Government-Business Cooperation National Case Studies* [in] *Security Through Innovation. Cybersecurity Sector as a Driving Force in the National Economic Development*, The Kosciuszko Institute, 2017, pp. 29–44.

28 Leitersdorf Y., Schreiber O., Reznikov I., *Trends in Israel's cybersecurity investments*, Crunch Network, 23/012017, https://techcrunch.com/2017/01/23/trends-in-israels-cybersecurity-investments/ [30 October 2017].

- Courses in product development, sales, operation scaling, user experience (UX), export strategies and the internationalisation of business;
- Providing opportunities for cooperation with mentors, i.e. experts in business with contacts and knowledge about the functioning of a given sector and the forms of support for companies;
- Providing access to the accelerators' network of contacts and potential business partners in both the private and the public sector and other investors within a given sector;
- An opportunity for startups to present their solutions during the demo day of the acceleration programme.

Acceleration programmes and support for cybersecurity startups are the foundations of Digital Innovation Hubs. An excellent example is the Canadian Global Cybersecurity Resource, which began as part of an acceleration programme at Carleton University. The nature of the cybersecurity market (a dynamically evolving landscape of threats, technological progress and a development model that is based on high-risk operation) makes it necessary to develop diverse forms of expert support for companies.

Building relationships with large companies

An important factor in the successfulness of Digital Innovation Hubs is a skilful building of relationships with the private sector, that is, the national ICT leaders, global corporations and state-owned enterprises. On the one hand, private companies can benefit from the technologies developed within the Digital Innovation Hubs (in the one-stop-shop formula), become their business partners or investors or develop their competencies by collaborating with academic institutions. On the other hand, private companies are able to offer startups unique conditions for the testing of innovative implementations (such as the National Cyber Testbed program of the Hague Security Delta in the Netherlands), the development of business competencies, or the establishment of numerous international contacts. The participation of large companies with a stable market position and reputation would also help to build trust in young innovative companies, for which a lack of an appropriate track record and experience (which are particularly significant in such a sensitive sector as cybersecurity) forms a barrier to development.

International cooperation

Due to the nature of cyber-threats and the interdependencies, extraterritoriality and intensification of cross-border business contacts within the modern digital economy, Digital Innovation Hubs need to develop international co-operation. Similarly to how governmental bodies communicate (e.g. as part of the NIS Cooperation Group, Group Global Commission on the Stability of Cyberspace, Global Forum on Cyber Expertise or Confidence Building Measures within the Organization for Security and Co-operation in Europe), support centres for cybersecurity innovation should maintain contact, cooperate and share information with one another. This is the purpose of the Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity (Global EPIC), which associates 14 entities from 10 countries. The aim of Global EPIC is to glocalise, that is, develop international cooperation between regional ecosystems by operating on the local level and promoting the best local solutions throughout the world. Global EPIC is focuses on 10 priority areas, including investment support, sharing of business services and expert resources, education or analysis of new trends on the market.

Participation of public administration

Public administration, as the leader of the national cybersecurity system, should participate in Digital Innovation Hubs. This includes bodies of local self-government and regional administration (as part of the regional ecosystem), as well as the central government. As the experience of global leaders in cybersecurity (the UK and Israel) shows, the sector cannot develop without the state's engagement in both the civilian and the military domains. The state should support the development of the cybersecurity sector, from carrying out cybersecurity strategies, through creating mechanisms for cooperation, to drafting R&D programmes. Consequently, Digital

Innovation Hubs should engage the representatives of public administration on many dimensions of their operation. In the case of the Israeli CyberSpark, the state supports it not only by allowing access to infrastructure, but also through economic and fiscal benefits. In the UK, the Government Communications Headquarters is the co-creator of an accelerator programme for innovative startups[29] and the Cyber First educational programme. Public administration can benefit from the development of a Digital Innovation Hub, both in terms of acquiring technologies that increase the IT security of a given organisational unit and the long-term implementation of the state pro-innovation policy.

Furthermore, support for Digital Innovation Hubs is part of both the 'Strategy for Responsible Development' with respect to both the implementation of the developmental programme for Cyberpark Enigma and the National Cybersecurity Policy Framework of Poland for 2017–2022. One of the particular aims of the latter is to develop the national industrial and technological resources for the benefit of cybersecurity.

The Polish experience: the CYBERSEC HUB

The CYBERSEC HUB, created by the Kosciuszko Institute, is the first centre for cybersecurity competence and innovation in Poland. Since 2016, taking advantage of Krakow's unique potential (its academic environment, high IT competencies, international corporate security operations centres and a robust startup ecosystem) a network structure, which includes the representatives of the local public administration, universities, business institutions, expert community and technological companies has been established to support the development of SMEs and startups that create cybersecurity solutions as part of. The CYBERSEC HUB focuses on eight priority areas:

1) The introduction of cybersecurity into university curricula (AGH University of Technology, Krakow University of Technology and Jagiellonian University);

2) Stimulation of the development of innovative cybersecurity products and services through real living labs;

3) Support for the internationalisation of startups and SMEs that offer cybersecurity products and services;

4) Stimulation of joint research and education among the regional businesses and companies;

5) Support for the development of the internal market by matchmaking the consumers and the regional providers of cybersecurity products and services;

6) Establishment of an knowledge hub on the cybersecurity market in the form of a one-stop-shop;

7) Encouragement of international investments in cybersecurity;

8) Establishment of a centre of excellence in cybersecurity, with an interdisciplinary department for research on cybersecurity.

Programmes and events that have been carried out as part of the CYBERSEC HUB include:

- CYBERSEC ACCELERATOR programme supporting the internationalisation of seven innovative startups and SMEs from the Lesser Poland Voivodeship through participation in economic missions to the US, Israel and UK, promotion during the 2nd Polish Cybersecurity Forum and the 2nd and 3rd European Cybersecurity Forum (CYBERSEC HUB expo), expert mentoring in export strategy and facilitating contacts with investors;

- Organisation of the Future Stream during the 2nd and 3rd European Cybersecurity Forum, dedicated to the development of innovation and investments, international cooperation and the promotion of technologies created by startups;

29 Forbes, *First Cybersecurity Startups Graduate from the UK Intelligence's GCHQ Accelerator*, 25 April 2017, https://www.forbes.com/sites/montymunford/2017/04/25/first-cybersecurity-startups-graduate-from-the-uk-intelligences-gchq-accelerator/#74fd8c5963de [30 October 2017].

- Many industry events facilitating business contacts, such as conferences and meeting with local partners (e.g. the European Enterprise Network or startup ecosystem organisations), the Cybersecurity Evening at the Polish Embassy in London aimed at promoting Polish solutions in the UK or participation in a Polish governmental economic mission to the US;
- Visits by foreign and national investors to the institutions of the local startup ecosystem;
- Publication of the 'European Cybersecurity Market' quarterly, dedicated to the evolution of the European cybersecurity market, European startup ecosystem and innovative technologies, and publication of the *CYBERSEC HUB Innovation Book* promoting solutions created by local start-ups and SMEs;
- Establishment of the Cybersecurity Centre of AGH University of Technology and discussions concerning the expansion of cybersecurity in the educational offer among universities in Krakow;
- Inauguration of Global EPIC, which was co-created by the CYBERSEC HUB (Kosciuszko Institute);
- Meetings with the representatives of the local and central administration and leading technological companies concerning the development of regional specialisation in cybersecurity.

Public task co-financed by the Ministry of Foreign Affairs of the Republic of Poland under the Public Diplomacy 2017 competition and the component „The civil and municipal dimension of Poland's foreign policy 2017".

The publication presents opinions of its authors and cannot be equated with the official position of the Polish Ministry of Foreign Affairs.

Ministry
of Foreign Affairs
Republic of Poland

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000. The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

The Kosciuszko Institute organizes European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.

Office: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: instytut@ik.org.pl

More on the European Cybersecurity Forum: http://cybersecforum.eu/

Further comments: Magdalena Bujak, magdalena.bujak@ik.org.pl, tel. +48 12 200 23 69