VOL 1 (2017) ISSUE 4

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

European Cybersecurity Market is a new publication designed to promote innovative solutions and tools in the field of cybersecurity. In order to raise awareness and increase cooperation in the developing digital economy, this periodical will be openly distributed to all interested parties and stakeholders.

ISSN: 2543-7259

European Cybersecurity Market is a quarterly publication.

THE KOSCIUSZKO INSTITUTE

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: robert.siudak@ik.org.pl

www.ik.org.pl
www.cybersechub.eu

CO-FINANCED BY

European Funds
Regional Programme

KRAKÓW REGION
MAŁOPOLSKA

European Union
European Regional Development Fund

FOREWORD

ROBERT SIUDAK
Chief Editor of European Cybersecurity Market
CYBERSEC HUB Project Manager
Research Fellow of the Kosciuszko Institute, Poland

Cybersecurity is a global challenge which we have to tackle both globally and locally. Building regional ecosystems enables strong and efficient cooperation between university centres for research and innovation, large international companies, local SMEs and startups. The synergy that develops between those stakeholders allows for the accumulation and unfettered flow of knowledge, good practices and key competences. Education and training of world-class specialists and innovators through university courses and participation in private-sector initiatives fosters the development of medium- and long-term research projects. It also encourages investment in promising technologies at the early stages of their development. In turn, an innovative sector of products and services can grow on this foundation of basic and applied tasks.

It is my great pleasure to present you with this special edition of European Cybersecurity Market that is focused on regional cybersecurity ecosystems. Inside, you will find contributions from local centres across a wide geographical range: from the French Pôle d'excellence cyber through the Canadian Institute for Cybersecurity and the Dutch Hague Security Delta to the Polish CYBERSEC HUB. All the presented ecosystems are unique in some way, but they all share the same need for tighter international cooperation. One of the answers to this challenge is the Global EPIC platform, which is profiled in one of the articles included in this issue.

I hope you will find interesting articles to read in this edition. I wish they encourage some of you to contribute to your own regional ecosystem by supporting R&D and cybersecurity education at the local level.

Robert Siudak

CONTENTS

5 SELECTED REGIONAL INNOVATION CENTRES FOR CYBERSECURITY
Robert Siudak in collaboration with Global EPIC

14 EUROPEAN REGIONS ARE ON THE FOREFRONT OF CYBERSECURITY COOPERATION
François Fleith

22 POLAND TODAY – THE PLACE AND TIME TO LAUNCH YOUR CYBERSECURITY START-UP
Bartosz Józefowski

30 INTERVIEW
with Martin Sebena

33 THE CANADIAN INSTITUTE FOR CYBERSECURITY PROTECTING GLOBAL CITIZENS IN THE CONNECTED COMMUNITY

39 THE HAGUE SECURITY DELTA: THE DUTCH METHOD OF COLLABORATION AND INNOVATION FOR SECURITY
Richard Franken

SELECTED REGIONAL INNOVATION CENTRES FOR CYBERSECURITY

Cybersecurity threats are a global challenge disrupting local modern living. Hardly a day goes by without news of yet another harmful attack, which suggests that our current approaches to cybersecurity are failing.

AUTHORS:

Robert Siudak, The Kosciuszko Institute

In collaboration with Global EPIC:

Anat Karmona, CyberSpark

David Crozier, Centre for Secure Information Technologies

Dan Craigen, Global Cybersecurity Resource

Darin Andersen, CyberTECH Network

Richard Franken, The Hague Security Delta

Cybersecurity threats are a global challenge disrupting local modern living. Hardly a day goes by without news of yet another harmful attack, which suggests that our current approaches to cybersecurity are failing. Isolating cybersecurity as its own "special domain" ignores its inherent presence in all sectors and on all levels of society. Consequently, new approaches need development if we are to achieve the global and local benefits offered by cyber and cyber-enabled technologies. The leading competence and innovation centres for cybersecurity are established all around the world in the form of regional hubs. This article presents a list of selected innovation centres for cybersecurity.

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

[1] Israel's National Cyber Bureau data. (8) HM Government, *The UK Cyber Security Strategy 2011-2016: annual report*, 14 April 2016, 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; (online) 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).

[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).

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 and post-quantum cryptography.

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 invertors 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, 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];

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

[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).

- 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, 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;
- 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.

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

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 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;

[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-kansennederlandse-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 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).

- 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.

CYBERSEC HUB (Poland)

CYBERSECHUB

Poland's abundance of cyber talent has been proven by numerous rankings and hackathons. Polish developers and hackers have won almost every well-known cyber contest from Locked Shields (2014) through Capture the Flag cycle (2014) to the 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[11]. Drawing upon the world-class human resources, Cybersecurity might become one of the most globally competitive sectors of the Polish economy.

In order to support this specialisation, over twenty stakeholders from Kraków, Małopolska Region, formed the CYBERSEC HUB coalition. Their goal is to create a local ecosystem that will help to harvest accumulated technology in the Research and Innovation Centre on Cybersecurity. Kraków is one of the largest startup hubs in Central Europe with over two hundred regional ICT businesses and several global IT companies, many of whom have already moved their R&D and Security Operations Centres to Małopolska. Hub activities coordinated by the Kosciuszko Institute are supported both by central and regional authorities, such as the Polish Ministry of Digital Affairs, the Municipality of Kraków, and the Marshal Office of the Małopolska Region.

CYBERSEC HUB provides a wide range of cybersecurity opportunities for companies, from education and training, R&I possibilities, to the development of innovative products. Amongst them:

- Cybersec Accelerator programme – designed for regional cybersecurity startups/SMEs in order to help them internationalise and scale their offer;
- Economic missions – organised for entrepreneurs and researchers who plan to expand to foreign markets (already organised for the USA, Israel, the United Kingdom);
- Workshops, conferences, trainings – enables transfer of knowledge, networking, and community building activities;
- One-stop-shop – tailored offer for micro/small/medium/scale-up companies, including products and services from both SMEs/startups and large enterprises from the region;
- Higher education programmes – offered by the Cybersecurity Centre at the AGH University of Science and Technology and IT department at the Cracow University of Technology.

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

[11] Hacker Rank, Which Country Would Win in the Programming Olympics?, 2017, [online] www.blog. hackerrank.com/which-country-would-win-in-the-programming-olympics/ (access: 16/10/2017).

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 inaugural meeting of Global Epic at CYBERSEC 2017 in Krakow.

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).

The article is a part of a publication „Regional innovation centres and their role in dealing with cyber disruption" that is a 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 the opinions of its author and cannot be equated with the official position of the Polish Ministry of Foreign Affairs.

Ministry
of Foreign Affairs
Republic of Poland

CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

Brussels 27. 02. 2018

EUROPEAN CYBERSECURITY FORUM CYBERSEC

DEALING WITH CYBER DISRUPTION

BRUSSELS LEADERS' FORESIGHT

EUROPEAN REGIONS ARE ON THE FOREFRONT OF CYBERSECURITY COOPERATION

BY FRANÇOIS FLEITH

1. Pôle d'Excellence Cyber

As outlined by the study conducted by the consulting firm Optimity for the European Commission on *Synergies between the civilian and the defence cybersecurity markets*[1] , "some of the leading Member States have started to develop regional technological clusters of excellence (e.g. the UK, France, and Finland). These clusters aim to leverage the technological potential and link national authorities, academia and industry to develop innovative solutions, including cybersecurity solutions."

The Pôle d'Excellence Cyber in France is an example of a cluster that was created regionally, in Bretagne, with a nationwide spread.

Bringing Capabilities Together

Set up in 2014 under the aegis of the French Ministry of Defence and the Regional Council of Bretagne, the Pôle d'Excellence Cyber operates nationwide and aims to extend its scope internationally. It is clustered around the Ministry's actors, which rely on Bretagne's academic and industrial network, as well as national and foreign partners. The roadmap of the Pôle d'Excellence Cyber is to boost the development of:
– the offer of cyber training (basic, in-service, and higher education),
– academic cyber research,
– the Cyber Technological and Industrial Base, with special regard to innovative SMEs-SMIs and their access to international markets.
The Pôle d'Excellence Cyber addresses 3 major challenges, for the benefit of the French cyber defence and cybersecurity communities:
– offering the appropriate skills for the development of the cyber industry,
– offering a panel of research coherent with the needs of the Ministry and the industry,
– offering trusted solutions and services.

PÔLE D'EXCELLENCE CYBER

[1] https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets

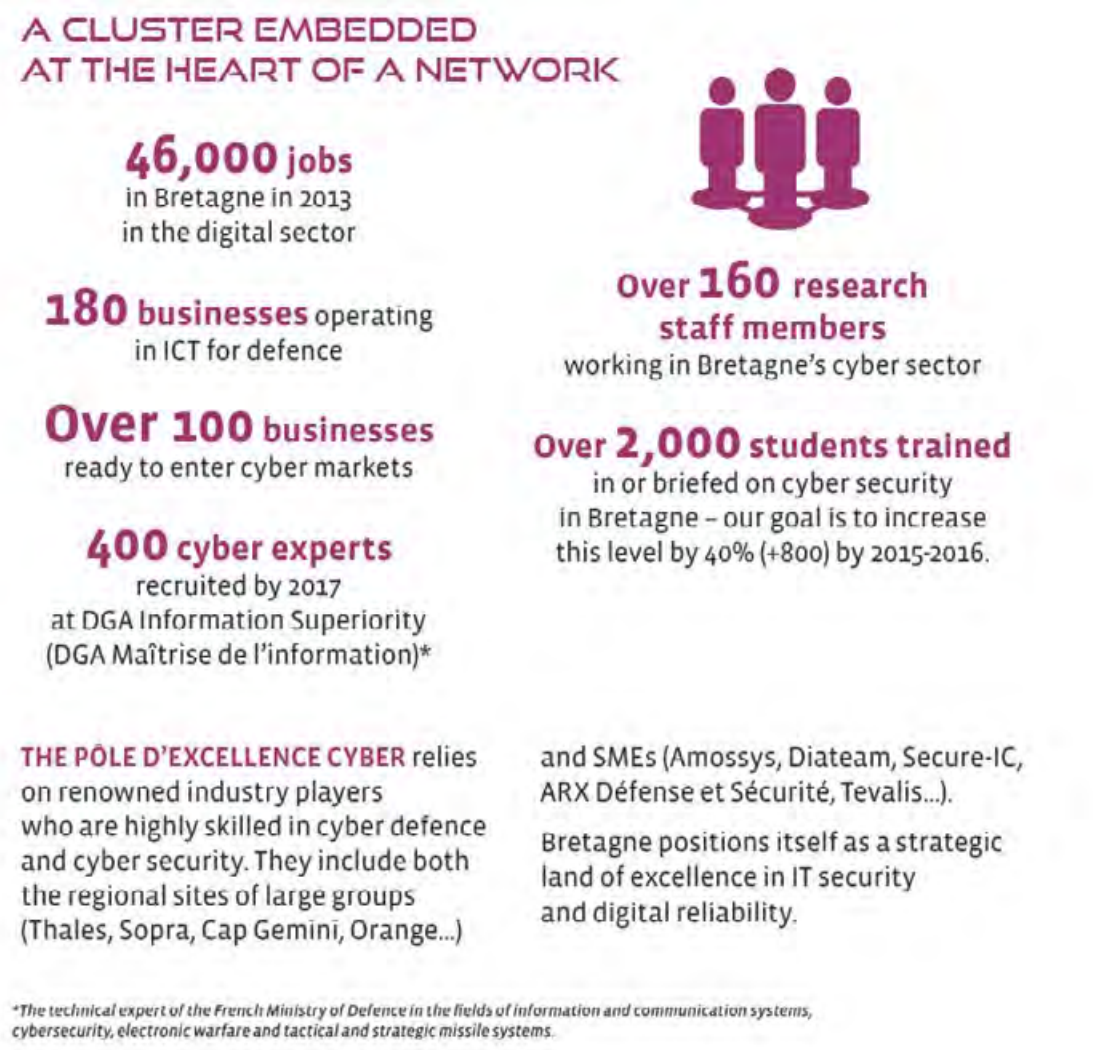
A Collaborative and Networking Organisation

As a non-profit-making association, the Pôle d'Excellence Cyber brings together civilian and military, public and private, academic and industry key players, drawing on their respective skills and areas of expertise. Thematic expert groups and working groups (training, research, industrial development, platforms, frame of reference, etc.) bring together all members and partners of the Pôle. This pragmatic approach allows a better interaction and cooperation within the cluster, thus remaining coherent, effective, responsive, and operating in project mode.

As of now, in the applied research field, the Pole d'Excellence Cyber has created four industrial research chairs on cyber defence, naval systems, threat analysis, and critical infrastructure protection.

There are more than 20 new training programmes, among which a master's degree specialised in cyber defence conduct of operations and crisis management. A budget of €12M is granted over a 6-year period to research theses, post-doctorate levels and scientific seminars; €6.3 M is invested in research studies and in the procurement of training platforms.

The Pôle d'Excellence Cyber has now more than 30 active members from training, research, and economic development sectors, as well as the Ministry of Defence, with over a dozen major industries, such as Airbus Defence & Space, Amossys, Atos-Bull, Bertin, Cap Gemini-Sogeti, DCI, DCNS, EDF, La Poste, Nokia, Orange, Sopra Steria, Thales…



2. The Cyber Week

As a region at the cutting edge of cyberdefence and cybersecurity, Bretagne has organised and hosted in November 2016 the first "European Cyber Week". This high-level event, sponsored by the cyber cluster Pôle d'Excellence Cyber, has featured a week-long agenda brought by key cyber stakeholders from both France and Europe.

This event was intended for cybersecurity communities including startups, small businesses, industry, research, and academia[2]. For this first representation of the European Cyber Week in Rennes, more than 1,200 participants were registered over the week; 10 European regions were represented and more than 400 students participated in the Hacking challenge. The Symposium on European Regional approaches for dual-use cybersecurity strategies[3] was organised during the Cyber Week in Rennes was targeting European Regions, Development and Innovation Agencies, clusters, and businesses.

The subject was introduced by Paul Anciaux, Policy Officer Defence Industry at European Commission (DG for Internal Market, Industry, Entrepreneurship and SMEs), who gave a complete insight on how regional authorities and SMEs can leverage on dual-use technologies to "maximise their investments in R&D, to enhance niche specialisation or simply to support the sectorial diversification of regional enterprise with a view to sustaining activities or creating new jobs."

The objective of this "peer-review" between regional authorities, clusters, and businesses was to exchange good practices on cybersecurity strategies in the area of dual-use technologies.

Cyber Week Programme

- **C&ESAR Conference:** state of play of technological advancements in cyber defence and cybersecurity. Audience: researchers, engineers, information system directors, military and civilian personnel Organised by the French Ministry of Defence.
- **EIT Digital symposium:** bringing together research and cybersecurity firms. Audience: businesses and labs. Organised by EIT Digital represented in Rennes by IRISA and INRIA.
- **EEN business meetings:** B2B and mix-and-match meetings between businesses and research labs, between businesses and investors, between SMEs and large corporations. Audience: SMEs, corporate groups, labs. Organised by Bretagne Development Agency (BDI) and the European Enterprise Network.
- **Symposium on cyber-security strategies:** sharing best practice among European regions for cybersecurity strategies on dual-use technology. Audience: European regions, businesses, clusters. Organised by the European Union and Bretagne Regional Council with BDI.
- **Invest in cyber:** Networking opportunities between startups in their fundraising stage and investors. Audience: startups and investors. Organised by Images & Réseaux cluster.
- **"Capture the Flag" challenge:** open to students only. Organised by Airbus D&S, Thales group and Telecom Bretagne.
- **Symposium on Smart Grid cybersecurity:** state of play of research in the field of smart grid cybersecurity. Audience: cybersecurity and smart grids researchers. Organised by SEE (a French learned society specialising in electricity, electronics, and ICT).

[2] http://european-cyber-week.eu/

[3] EU funding for Dual Use - A practical guide to accessing EU funds for European Regional Authorities and SMEs: http://ec.europa.eu/DocsRoom/documents/12601

Peer-review: "Dual-use implementation across cybersecurity strategies"

The workshop was moderated by Mathieu Doussineau, S3 Platform, Growth and Innovation Directorate, JRC-European Commission. The peer-review workshop focuses on two key issues about developing a cybersecurity strategy and its dual-use aspects. Participants had the opportunity to exchange and learn from best practices in European regions.

Key issue 1: Research, education and business links. How to facilitate access of SMEs to these particular growth drivers and use them to develop dual-use activity?

Key issue 2: Improving access to public procurement and large groups for SMEs. How to facilitate access of SMEs to these particular growth drivers and use them to develop dual-use activity?

Results of the first panel discussions: It was a large panel with representatives from various countries: Portugal, UK, Estonia, Spain, Hungary, Poland, and France. The panel agreed on the fact that the two identified issues are fundamental and intertwined. The panel pointed out that it is extremely important to develop links between the triangle academia--education-business to make people work together on cyber, with a key focus on education considering the lack of qualified human resources available to work in the field of cybersecurity. However, it is also important to develop links with:

- financial institutions and instruments, taking into account the lack of funding for SMEs working on cybersecurity,
- government and defence agencies, considering their key role in buying cyber technologies.

Some participants underlined some difficulties to finance projects linked with dual-use technologies considering the different rules applying to the civil/military sector. Civil markets are open but military markets often are not: it makes the growth of SMEs developing cyber technologies outside their national market very difficult. SMEs working on dual-use technologies sometimes do not fit into legislation: it might be helpful to develop at the regional, national, or European level an instrument to facilitate their funding and development. The use of the European Regional Development Fund (ERDF) and Horizon 2020 funds for cyber should also be promoted and facilitated. The panel agreed on the fact that the implementation of the cybersecurity contractual Public-Private Partnership under the lead of the European CyberSecurity Organisation (ECSO)[4] is an important tool. They also recognised that a bottom-up approach behind the ECSO is crucial. In order to make ECSO work for SMEs, the panel found necessary to keep an easy procedure (such as through the cascading fund for third-parties used in other PPP). Finally, the participation of Regions within ECSO should help to guarantee easy access to SMEs and simplification.

Key issue 3: How to improve research education and business links?

Result of the second panel discussions (also a large panel with representatives from various European countries): A cluster is the best way to link research, education, and business in an efficient and productive manner. Europe has more than 200 identified clusters. The key question is to determine which cluster models work and which do not.

In the UK (e.g. Cambridge or Warwick), we have observed many Business and Science parks that were established to stimulate innovation. It is essential that research/education and business are brought together so that scientific knowledge can be translated into products and business creation. The role of incubators is to enable and support this translation from knowledge to business. At this point of business creation, technical and business risks are being assessed and need to be reduced in order to attract investors (business angels or private investment). At the same time, EC funding in R&I is a strategic tool to foster innovation and reduce technical risks through experimentation. The role should be relayed by the regions through their S3.

[4] European CyberSecurity Organisation https://www.ecs-org.eu/

Member states also have a role to play in supporting business creation, for example by allowing tax incentives to startups and entrepreneurs who are ready to take risks. Startups are encouraged to develop dual technologies (applicable to both civil and military markets). In doing so, they may benefit from additional funding from governmental agencies and could also gain access to testing their product/service. Finally, business and entrepreneurship education should be developed at schools and universities in order to reach a common mindset among the students.

During the peer-review. © C. ABLAIN

Key question 4: How to improve access to public procurement and large groups for SMEs?

Public administrations and large industrial groups have very different procedures in terms of procurement from SMEs. Legal obligations can also be very different. For example, in the UK (but also in other countries) we have quota for public administrations purchasing from SMEs. Practical information on how to deal with public procurement needs to be largely communicated to SMEs. It is the role of the clusters to disseminate information among its members.

Product qualification/certification is a big issue for SMEs. This is a costly and time-consuming process, especially when the qualification and certification processes are country specific. Within ECSO, a special Working Group is dedicated to proposing common criteria/standards for product certification to cope with the digital single market in Europe.

3. Further Cooperation in Europe

Based on the success of this first "peer review" between some regional authorities, clusters and SMEs, and the need for further cooperation in the field of cybersecurity, it was decided to extend the process and formalise a dedicated Working Group within ECSO in order to deal with the issue of cooperation between regional organisations.

First meetings between the European Commission and the interested regions have already been planned for the first semester of 2017 to set up the foundation of this cooperation. Many opportunities have been identified to attract other regions that could potentially be willing to join ECSO and participate in the Working Group.

The next European Cyber week in Rennes is planned for 27 November-1 December 2017. The organisers hope to attract more European delegations to the different events, as most of them are open to a large number of regional agencies, clusters, SMEs, and large industrial/services groups. This year, the "Catching the Flag" challenge will be largely open to students from various European universities and engineering schools, which makes it a real contest to elect and encourage the best talents in cybersecurity.

Bretagne, Europe's Cyber Valley

Bretagne is at the forefront of digital technology and has become a benchmark region in cybersecurity. Our ambition is to drive forward the cyber-defence and cybersecurity industry of France and Europe, drawing on our region's capabilities to do so. We are home to a thriving and innovative ecosystem of world-renowned firms, research teams from the best institutions, the Ministry of Defence cyber teams, as well as a number of prime contractors and cutting-edge SMEs. ■

ABOUT THE AUTHOR:

François Fleith is currently working as coordinator within the Pôle d'excellence cyber, created by the French Ministry of defense and the Brittany Region. Previously, as Director of innovation at Opticsvalley, he was supporting a cluster of innovative SMEs and startups in the photonics field serving various applications markets such as defense, security, health and medical. After graduated from Supelec in electrical engineering, and a first experience in R&D military telecom projects within Philips-TRT, he went to INSEAD where he got an MBA. He served as a French navy officer and had several positions as a reserve officer both on ships and within the Head of Staff. He was auditor at the Institute for Higher National Defense Studies

securing

MORE THAN SECURITY TESTING.

WHAT WE DO?

Founded in 2003. Since then we have supported leading banks, insurance companies, telecom providers, government institutions and software houses, providing services such as:

- **Application and infrastructure security testing**
- **Code review**
- **Definition of security requirements**
- **Project review**
- **Education**

KEY FACTS:

Founded in **2003**

Over **450 successful** security assessments in **17 countries**

More than **150 critical vulnerabilities** identified and removed

Verified systems manage critical infrastructure and process **millions of users' records**

Our research has been selected for leading security **conferences worldwide**

Customers: Banking, Insurance, Finantech, Software Houses, SaaS Vendors, Telecommunication, IT, Utilities, Industry, Public, Military

WHO WE ARE?

Team of experienced application security consultants. We are focusing on security aspects of applications and IT systems. Our expertise covers different kinds of applications (e.g. electronic banking, electronic payments, FOREX, e-commerce, home/office automation, surveillance, voting, internet of things, etc.) and wide spectrum of technologies (web, mobile, WebServices, embedded, desktop, SaaS, cloud).

We are constantly improving our skills and knowledge in order to stay on the edge of information security issues. This allows us not only to focus on past and current risks but also to look forward into the future. Examples of our research topics include: transaction authorization systems, banking malware, home automation, M2M communication, Bluetooth Low Energy, browser plugins, pull-print systems, proprietary protocols, HTML5 and many more.

KNOWLEDGE:

We are sharing our knowledge on many conferences and meetings. Our research topics has been chosen for leading security conferences worldwide such including: Black Hat USA 2016, OWASP AppSec Europe 2014-2016, Infosecurity Europe Intelligent Defence 2016, CONFidence Krakow 2014-2016, ZeroNights 2015, BSides London 2015, Black Hat Asia 2015, PH Days Moscow 2014, HITB Amsterdam 2014, Internet Banking Security Warsaw 2013, BruCON, Belgium 2012, Black Hat USA 2012 and OWASP, ISACA, ISSA meetings.

OUR APPROACH TO APPLICATION SECURITY TESTING:

The goal is to fix vulnerabilities.

- Our report always includes recommendations on how to fix discovered vulnerabilities.
- Support during fixing phase.
- We communicate with the tested solution vendor to help them understand problem and provide remediation.
- Additional tests after vulnerabilities are fixed.

The main aspect of security assessment is to take real risk impact into account.

- Prior to testing, we perform threat identification and threat modeling.
- We prioritize attack scenarios.
- We take into consideration business impact as well as business logic.

We say no to fire and forget tools.

- Automatic tools can only find small percentage of real vulnerabilities.
- The real threat is live attacker, not automatic tool.
- We prefer manual verification, using specialized “home-grown” tools.
- Understandable, customer-oriented report.
- Realistic and dedicated recommendations.

Deep technical knowledge and audit skills.

- We stay on the edge of new attack techniques and areas (own research, 0-days, worldwide conferences).
- We are certified experts of ITsec management and audit (CISSP, CISM, 27001, PCI DSS, ...)

MORE THAN SECURITY TESTING:

Security testing at very end of the project, just before (or after) deployment are still key component of achieving application security. Nevertheless, doing only security tests as a part of UAT is not effective, because significant costs of fixing bugs at late project stages. That’s why besides security testing, we offer support at each stage of development:

- Security training for developers and QA team
- Security requirements definition (functional and non-functional)
- Project reviews
- Code reviews
- Consultations
- Security tests

CONTACT:

info@securing.pl
tel: +48 12 425 25 75
fax:+48 12 425 25 93
www.securing.pl

POLAND TODAY

THE PLACE AND TIME TO LAUNCH YOUR CYBERSECURITY START-UP

BY BARTOSZ JÓZEFOWSKI

The Polish start-up sector has been developing dynamically for many years now, bringing both quantitative and qualitative improvements. Furthermore, the ecosystem has been maturing along with business environment institutions, public partners and private investors. In fact, Poland is an excellent place for launching start-ups in any industry sector, especially cybersecurity – right here and now.

The Market and the Needs

In 2004, the value of the global cybersecurity market amounted to approx. USD 3.5 billion. In 2017, the value was estimated at USD 120 billion with a 10% year-on-year growth potential. Nowadays, there are practically no aspects of life that would not involve the use of electronic devices and/or the Internet. The digital immersion will continue to grow, which is likely to result in an increase in the number of attacks and also – though indirectly – the growth of the value of the cybersecurity market. The Internet of Things, Industry 4.0, AR/VR, autonomous vehicles, artificial intelligence, e-government, remote solutions for the healthcare industry as well as the good old GPS, WiFi, social tools, online banking, e-commerce and m-commerce: these all do not only dramatically accelerate the development of civilization, but they also cause a major headache for those who are responsible for ensuring their security – top management, IT security departments and users.

From a start-up's point of view, it is critical to determine the market's potential, the needs of potential customers and the problems that need to be solved. At first, it is hard to escape two truisms: first, the scale of cybercrime continues to grow rapidly worldwide; second, Poland is just starting to close the gap within this industry. But it is not all that bad. In the cybercrime index prepared in 2017 by the International Telecommunication Union (ITU), Poland was ranked 33rd worldwide (leader: Singapore) and 16th in Europe (leader: Estonia). Nonetheless, there is still no reason to rejoice. In the period between May and August 2017, the public was informed about over a dozen of major cyber-assaults in Poland that affected the websites of the Parliament, the Government Legislation Centre, and the biznes.gov.pl portal.

The public sector awoke from its cyber-torpor in 2012. It was during the ACTA protests when some of the protesters joined – more or less consciously – the DDoS attacks aimed at the websites of numerous governmental agencies. In June 2015, the Supreme Audit Office published a post-control report entitled

"Protection of the security of cyberspace of the Republic of Poland tasks implemented by state institutions". Its conclusions were bitter: the actions were too few and too slow; there was a lack of resources, decisions, cooperation and procedures. The report also acknowledged the lack of fulfilment of statutory obligations in the area of computerisation of public administration offices. Since then, the public sector has been witnessing an abundance of cybersecurity initiatives.

Most of all, "National cyber-security strategy for Poland for the period 2017–2022" adopted in May 2017 confirms that cybersecurity will constitute one of the major projects for the Ministry of Digital Affairs. Therefore, it is worth quoting two sentences included in the document – both are important to IT security and start-ups:

1. *The government of Poland aims at investing in the development of industrial and technological resources dedicated to the needs of cybersecurity by creating conditions that would be favorable for the development of companies, science-research centres as well as start-ups with business activities based on creating new solutions, also in the area of cybersecurity.*

Cybersecurity in numbers worldwide:

In 2016, it was estimated that the amount of losses resulting from cybercrime would reach USD 3 billion in 2012. In 2017, the estimates increased to USD 6 billion.

The number of ransomware assaults on healthcare institutions will quadruple by 2020.

In 2017 alone, the White House's spending on combating cybercrime increased from USD 14 billion to USD 19 billion.

Half of the companies have no means to detect a well-advanced cyberattack. One of the main reasons for this (30% of indications) is the lack of response from tools.

According to estimates by Cisco (2017), 44% of cybersecurity incidents have never been studied.

2. *In order to equal the chances of Polish entrepreneurs on the global market and support the development of Polish businesses in obtaining digital possibilities, it was decided to create innovation hubs dedicated to providing complex services for both companies and start-ups.*

This looks promising.

While at the central level there is relatively a plethora of cybersecurity-related activities, the regional and local levels witness very few such actions. It is worth mentioning here the words of J. M. Czajkowski and A. Maciejewski; they were uttered in 2017, but they mirror the climate pictured in the SAO report from 2015: *14 out of 16 voivodes did not fulfill their obligations (...) regarding control of IT systems used by local self-government entities and their associations as well as in the self-governmental juridical persons and other self-governmental organizational entities either created or managed by such entities.*

In order to indicate the scale of threats, let us remind that currently in Poland there are 16 voivodeships, 380 powiats and 2,478 gminas – which translates into nearly 3,000 territorial self-government entities (excluding local government-owned companies). On the other hand, "National cyber-security strategy for Poland for the period 2017–2022" pays much more attention to start-ups than self-governments. In addition, "Cyberspace Protection Policy of the Republic of Poland", which was created four years ago, does not provide regions with much support and useful tools either. However, both those strategic documents impose ambitious and otherwise valid objectives.

Half of the local government units in Poland do not pay attention to the significance of cybersecurity. This is caused mainly by a lack of resources that ought to be dedicated, for example, to training employees.

Jan Maciej Czajkowski, Joint Central Government and Local Government Committee

This might indicate that the territorial self-government will be faced – as it already happened before – with maximum challenges and minimum resources when trying to achieve these goals.

Only 11% of self-governments underwent training in the area of cybersecurity in Poland.

Andrzej Maciejewski, Deputy chairman of the Local Self-Government and Regional Policy Committee

An important source of financing might be the Operational Programme "Digital Poland for 2014–2020" which forecasts in its Axis II E-government and open government that approximately PLN 950 million will be dedicated to the availability and quality of public e-services, digitalization of processes as well as the availability and usability of public administration resources. It seems that it will lead to the emergence of a potentially promising market for new equipment, software and process solutions as well as business models at regional and gmina levels.

Surroundings and Partners

Who can you count on? Paradoxically – the Polish government, due to its efforts to build a favourable climate for both start-ups and cybersecurity. You can be sure to count on business environment institutions as they take their mission rather seriously. Nonetheless, there are a few cybersecurity start-ups in Poland and all BEIs (Business Environment Institutions) are willing to support. Last but not least, you can always count on the start-up industry itself. It is not only experienced but also very open.

Nevertheless, the fact is that the Polish IT security start-ups are scant. The obvious disadvantages of this are a lower level of market opportunities and lesser competition.

Resources

Is there a blueprint for building a successful cybersecurity start-up? Definitely yes; however, there is also a "but".

As for the key resources, people rank the highest. Poland has an extraordinary potential with excellent specialists in mathematics, engineering and programming. That is why hundreds of companies decide to launch their R&D offices here. We are also still competitive in terms of price. Nonetheless, the main advantage of our country is the quality of education and the continuously high work ethics. However, there is one "but" mentioned earlier. While the popularity of computer science studies continues to grow, the number of graduates has been plummeting unfortunately. This is the result of the "demographic tsunami" that has been forecasted since 2011.

Polish programmers enjoy an excellent reputation that has been confirmed by a plethora of successes.

The Polish national team has been participating in "LockedShields" - international exercises organized by NATO Co-operative Cyber Defence Centre of Excellence in Tallinn - since 2014. The team is issued by units subordinate to: Inspectorate of Information Systems, Resort Centre for the Management of Information Projects, Military University of Technology, the Internal Security Agency, CERT Poland, Polish Police Headquarters, Military Gendarmerie Headquarters, Military Counterintelligence Service, Centre of Cybernetic Operations and National Cryptology Centre. In subsequent years, Poland occupied the first, third and twice 6th place respectively amongst 25 participating teams.

Furthermore, in HackerRank based on the evaluation of the work of IT specialists, Poland occupied the third place in the general ranking of the best developers. Poland also came third – and rightly so – in the category "Which country never gives up?" which focuses on perseverance in problem solving. As the organizers summed up:

If we held a hacking Olympics today, our data suggests that China would win the gold, Russia would take home the silver, and Poland would nab the bronze.

The situation will get even worse in the coming years. Hence, the estimates already indicate that Poland will suffer from a lack of 30–50,000 computer scientists in different specialty areas. The HR departments of software houses already bend over backwards in order to meet the needs of their companies. Nonetheless, this is a problem that small companies, including start-ups, have been experiencing as well.

However, people are not the only critical asset. Think about the location for your office. In geographic terms, strong locations include cities such as Warsaw, Kraków, Gdańsk, Poznań and Wrocław. They are large urban centres with strong and vibrant start-up communities. They offer a wide array of office space: from strictly commercial space, to financed technological incubators, science and technology parks, all the way to co-working spaces. Part of this infrastructure was designed strictly with the start-up industry in mind.

There is a gap within the start-up ecosystem though. It results from the lack of incubators and accelerators that would resemble the American MACH37 or the British CYLON, both specialised in supporting cybersecurity start-ups; however, it can reasonably be assumed that the creation of such an incubator and/or accelerator is only a matter of time.Finally, the last critical resource to mention can be described as a mix of know-how, entrepreneurship and bold visions. The evaluation of Poland's potential in this area can be based on the observations of its start-up arena, which is not that bad at all. Polish start-ups are able to develop interesting solutions, extraordinary and effective business models, but most importantly easy to use and reliable products.

Financing

Let us take a closer look to the possibilities for financing available to cybersecurity start-ups. It is important to note the general favourability and openness of the public sector, especially the government, towards the development of innovative entrepreneurships, i.e. start-ups and computer security as a whole, as mentioned above. This is vital due to its influence on finances.

Of course, the deliberations ought to start from the EU funds as the pace and dynamics of the development of the Polish start-up sector will strictly correlate with further EU budget prospects and competition schedules.

It is also worth mentioning the launch of the Polish Development Fund (Polski Fundusz Rozwoju, PFR) which contains a consolidated support system dedicated to start-ups. The PFR is the flagship of a wider governmental program "Start In Poland" which plans to spend PLN 2.8 billion on the development of start-ups from the Smart Growth Operational Programme 2014–2020. The PFR's main instruments include the PRF Venture fund which consists of five tools dedicated to VC and CVC funds. The purpose of those funds is to capitalise innovative companies like start-ups. The National Centre for Research and Development adheres to similar principles, thus introducing its financial instruments: NCBR CVC and NCBR VC. In this case, the field of B+R in financed projects is much more emphasized, compared to other investment schemes. This also refers to research commercialization which, from the point of view of cybersecurity start-ups, might be of crucial importance.

Bartosz Józefowski during CYBERSEC 2017.

Let us add that EU funds are not the only sources of financing for a start-up. It needs to be noted that particular competitions held under the Smart Growth Operational Programme, the Operational Programme Eastern Poland and Regional Operational Programmes offer additional possibilities. To avoid making hollow claims, let us add that when we write these words, the NCBR is calling and enrolling for the second edition of the programme "CyberSecIdent – Cybersecurity and e-Identity". Research focused on *technological solutions that facilitate co-operation and co-ordination of activities amongst different domains of cyberspace security with special focus on digital identity* can obtain even up to PLN 20 million worth of support.

EU funds are made up of both national and international resources. It is worth mentioning the EU Horizon 2020 programme which provides two funding streams: "Secure societies – Protecting freedom and security of Europe and its citizens" and "Leadership in enabling and industrial technologies". These funds are hard to obtain, but they also offer much higher return in monetary support and prestige.

When considering the possibilities of financing start-ups, including those engaged in the cybersecurity industry, one cannot forget contributions from private investors. Recent months have shown a clear offensive advance of the private capital such as Sebastian Kulczyk's inCredibles acceleration programme with investments worth of USD 60 million, VC TDJ Pintago Ventures launched by T. Domogała and the Israeli fund Pitango Venture Capital (with plans for at least PLN 210 million to be invested in the next decade), Fidiasz EVC – a fund established by Krzysztof Domarecki, or Witelo Fund of Funds launched by PZU with an investment budget amounting to PLN 100 million which started its cooperation with zAtomico, Evolution Equity Partners specialised in in the cybersecurity sector, as well as DN Capital.

That is not all. There are also international corporations that keep their fingers on the pulse and, in recent months, have launched and/or already have a well-developed offer for supporting start-ups and building an ecosystem. The most recognisable and most experienced ones include hub:raum from T-mobile, Microsoft's Startberry, Campus Warsaw from Google and PWC's Startup Collider.

Therefore, it is hard not to recognise that the last dozen or so months have brought a spectacular increase in financing tools available to start-ups in the cybersecurity sector. This, combined with the already available and traditional start-up financing tools like crowd funding, business angels, few VC funds as well as the all-present 3xF – Family, Friends, Fools, allows to assert that a cybersecurity start-up will surely and painlessly obtain financing. What is important is the fact that a wide range of financing instruments and their operators provide each start-up at any given development phase – from pre-seed to growth and expansion – with a chance to thrive.

It is also important to mention the so-called Small Innovation Act that came into force in 2017 and promotes tax credits for entities launching research and development activities. Furthermore, there is an abundance of similar instruments that provide indirect support which proves crucial for a start-up's budget.

Scaling

What is the growth potential and conditions for the development of cybersecurity start-ups? They appear favourable indeed. Mostly, all major actors that inspire the creation of cybersecurity start-ups are aware that the sine qua non of a start-up includes scaling and an entry strategy into the global market (in which, as we mentioned above, the needs are enormous and still continue to grow). This is important as it assures that nobody will inhibit the company's development. At the same time, the condition of the start-up ecosystem, especially in the biggest innovative centres such as Warsaw, Kraków, Gdańsk, Poznań and Wrocław, allows to take an optimistic approach towards the environment where such growth ought to take place.

Poland has a high potential for both building and testing various solutions: access to the Internet can be regarded as widely common; most of the population uses mobile devices; almost half of citizens uses mobile Internet while Poles tend to spend most of their

In Poland, 80.4% of households and 93.7% of companies have access to the Internet. 30.2% of citizens and 93.6% of companies use the services provided by e-Administration. Furthermore, one in every three companies places their orders online while one-third of large entrepreneurships use the cloud. Mobile Internet is used by 46% of the Polish population.

Poles spend 4.4 hours in front of the computer on average and 1.3 hours using mobile devices. Average Internet speed in Poland amounts to 10.6 Mb/s, while the number of active mobile phones is approx. 60 million. The Internet penetration within the population in Poland reaches 60%, while the number of social media users actively using mobile device is estimated at 10 million, which accounts for one-fourth of the entire population. 94% of Poles use mobile phones, smartphones – 59%, laptops and PC – 77%, tablets – 24%, smart TV – 13%, e-Book readers – 2%.

days online. Computers, laptops, smartphones, tablets, or the Internet – they all have become an integral part of Poles' everyday lives, both at home and work.

Therefore, there is a starting point from which to build potential for global development.

Conclusions

Given the current pace and directions of the development of our civilization, there can be little doubt of the importance of computer security. As Ginni Rometty, the President at IBM, once asserted: "Cybercrime is the biggest threat to any company worldwide". Unfortunately, there is not much that can change it in the nearest future.

One cannot help but get the impression that Poland has accumulated factors that would contribute to the inundation of cybersecurity start-ups: the government administration and self-governments are maturing (in terms of awareness, decision-making and operations); the scale and scope of threats is growing; the start-up ecosystem continues to grow along with the range of possibilities for financing, and the demand thrives on all sides...

One could metaphorically say that in a puzzle of 1,000 elements, 999 have already been set in the right place. This is the part of the game where one can no longer conjecture, check, or consider. Clearly, 999 elements are more than enough to show what is missing.

Thus, is there someone who dares? ■

ABOUT THE AUTHOR:

Bartosz Józefowski – head of KPT ScaleUp acceleration programme, Board Member in seed investment fund, helping startups for 5 years, expieri-enced in all stratup support processes: incubation, acceleration, investment. Involved in #omgkrk and Startup Poland Foundation.

VoicePIN.com is a voice biometrics producer that developed a software for voice authentication for any application. Founded in 2011, Voice PIN replaces traditional passwords and pin numbers with natural voice commands. Its SaaS technology has been used by corporate customers from ING to Alior Bank and made it to the Top 10 at TechCrunch Disrupt competition in San Francisco last year. The Polish company, based in Cracow, is expanding in an emerging market and is focusing on the global development of the business by building a chain of partners on all continents. In 2016, Voice PIN opened a branch in Silicon Valley with plans to open others.

GET TO KNOW VOICEPIN

VoicePIN is the latest tool in biometric technology and speech recognition for data protection. Your clients and users can log on in a convenient way, without the need to
remember PINs and passwords. User verification becomes amazingly simple. Natural voice commands are all that is needed. VoicePIN minimizes the risk of frauds and personal data theft. The human voice is as unique as a fingerprint. VoicePIN saves you money by shortening client service time as well as enhancing the service and clients experience.
Thanks to our API, connecting VoicePIN to any mobile application, website, Call Center system, or an IVR is as simple as can be. VoicePIN can also be applied wherever there is no keyboard – in the dynamically developing Internet of Things.

The innovative technology enables voice recognition to be used for verification, access control, fraud detection and other security protection. It can be implemented on mobile apps and at call centers, helplines, websites and anywhere password-protected information exists. No automatic speech recognition software or hardware is needed therefore installation is fast and it's easy to use.

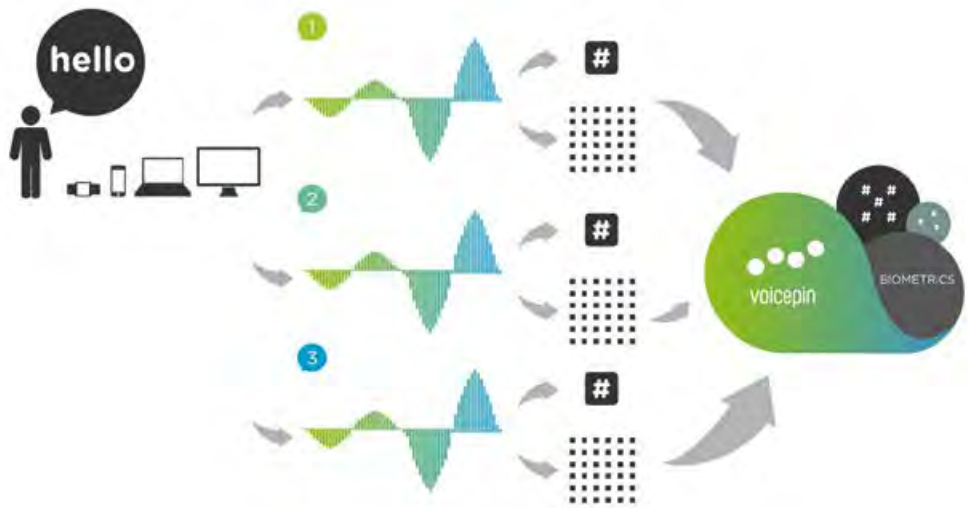
VoicePIN can be used to login, authorize transactions, reset passwords and perform many other security functions.

As the latest tool in biometric technology and speech recognition for data protection, users can log on conveniently without needing to remember pins and passwords. Natural voice commands minimize the risk of cyber-attacks and personal data theft because the human voice is as unique as a fingerprint which is carefully analysed and detected through Voice PIN's cutting-edge technology. Upon initial installation, a user registers a "voiceprint" which is stored in the form of mathematical models. Each time the user attempts to access protected information, the command is compared to registered voiceprints and the software verifies whether the voiceprint belongs to the user who registered it. Since individuals are identified by analysis of the voice, Voice PIN is a safer and less complicated alternative to traditional methods of authentication.

Voice PIN can be used to login, authorize transactions, reset passwords and perform many other security functions which is why the tool is currently being used in the financial sector, insurance industry and telecommunications. Businesses can subscribe to Voice PIN as-a-service and enhance their customers' user experience by providing hands-free authentication without logins or passwords. API integration is simple and does not require an installation process and can be used on multiple channels. This solution is the most cost-effective while providing high-level security.

While no biometrics tool can provide 100 percent safety, according to the company, Voice PIN is 98-99 percent effective. Passwords, pins, security answers can be obtained by unauthorized users but voice biometrics is good at detecting attempted fraud and provides a higher level of security than even more methods such SMS authorization.

Even though VoicePIN, in order to guarantee top-level security, uses complex, advanced technology, registration process takes about 15 seconds and the verification just 3 seconds!



A software producer invented a tool that enables users to login and verify their identity using only the sound of their voice.

WANT TO KNOW MORE?

Feel free to contact us:
VoicePIN.com
Krakusa 11 St.,
30-535 Cracow
+48 12 378 98 21
info@voicepin.com
TT: @VoicePINcom

INTERVIEW WITH MARTIN SEBENA

Martin Sebena discussed cybersecurity business trends with Robert Siudak during the third edition of the European Cybersecurity Forum, CYBERSEC 2017.

Robert Siudak: Do you believe that cybersecurity might be the next FinTech, when it comes to the market, when it comes to opportunities for new companies?

Martin Sebena: That is a great question, Robert! To answer it, I will go a little bit back in history to look at what happened to FinTech. FinTech is not a new thing. It has been here for forty to fifty years. SWIFT in the seventies: this was a FinTech. Bloomberg has been around for decades. But what really facilitated the growth and explosion of FinTech were two things. One was the advancement in technologies, and the second was the global financial crisis. Because of the global financial crisis, lots of companies came in and said: "we are going to do things differently". Comparing this to cybersecurity nowadays makes sense. You have the same rapid advancement of technology that is precipitating the growth of the cybersecurity industry. Perhaps we have not had the breakthrough event yet, that, like the global financial crisis in FinTech, would bring attention to cybersecurity. But the last year or even this year can prove to be the transforming period, because you have these government hacking scandals, breaches and a lot of incidents that call the attention of regulators, of governments. Well, it is witnessed even by the presence of the Polish Prime Minister today at the opening ceremony of CYBERSEC 2017.

Now, you have the top-down attention, the push by the governments for more cybersecurity, for more development in this area. Cybersecurity is indeed in this moment where you have "bottom-up push", that is the companies we have seen here today during the Pitch Deck Contest – as well as a top-down push for more cybersecurity.

So, yes, there is a strong demand. Cybersecurity is probably at the cusp of something huge. One more thing that I would add is that FinTech is more of an 'umbrella term', like a catchall phrase. If you have a closer look at it, this umbrella covers a number of areas: RegTech, InsurTech, etc. Pure FinTech is then not as big as it seems, and CyberSec might be seen as catching up very quickly.

R.S.: Let's talk about the different attitudes towards cybersecurity, and generally about producing

a cybersecurity product and introducing it into the market. You have experience in the Asia-Pacific Region, and you are originally from Central-Eastern Europe. So how do you see the perspectives of these two regions? What are the main differences, is there a global common point?

M.S.: Let's say that the first and foremost thing is that Asia is much more heterogeneous. In Europe, we are all different, but at the same time there is the European Union, there is much common legislation, it is much closer, country to country, while in Asia you see a lot of differences. You have countries like Singapore, Hong Kong, and Australia that are very open, very supportive of new technologies – also cybersecurity – that support startup ecosystems.

On the other side, we have countries like Korea and Japan, perhaps surprisingly for some of you – these countries do not support the startup scene. And in this way, they are doing harm to themselves, because the technologies are not developing within these countries and they will have to catch up later. So, they are lagging behind. You also have countries in the middle, which are probably Southeast Asian countries and the special case of China. Just to elaborate a bit more on China – this tends to be a very difficult environment for the outsiders. China tends to pick up certain industries that they want to push, in which they want to be the leader. So, if your startup is within that industry, you are going to experience a huge boost.

Furthermore, there is a difference on the regulatory-legal side, as well as a difference on the commercial side when it comes to the APAC region. Again, let me start with China. They basically have four different characteristics. The first one will be speed: you have to be fast in China. If you want to be successful, you have got to be fast, because – number two – competition is huge. The other startups that you are against within China are trying to copy what you have. They are very quick at replicating. You think that you are successful – but is your position permanent?

Others will have the same thing in 2-3 months. So, if you want to be in these countries, you need to be very, very, very fast. And that brings us to number 3, which might probably be an obstacle for some – the scale. On one hand, that might be a good thing. In China or in Asia in general – because these are very populous markets – you can achieve scale, a huge scale, a scale you cannot achieve in Europe. But on the other hand, are small startups ready for that scale? Do they have the resources to put into it, to sustain a high scale?

Martin Sebena is a Startup Mentor specialized in the Asia-Pacific region, where he has over seven years of experience in leading business development for FinTech companies. He is currently working with a Hong Kong-based InsurTech startup, CoverGo, where he directs business development and strategy. At the same time, he is participating in three accelerators across the region. Previously, Mr. Sebena worked with FinTech companies to set up operations centres in Hong Kong and grow business development in APAC.

In China or in Asia in general – because these are very populous markets – you can achieve scale, a huge scale, a scale you cannot achieve in Europe.

These are the issues companies have to think about. And the fourth thing is monetisation. If you are focused on a retail customer, or if you are doing B2C business, you are able to monetise, to get money very quickly, and that is because the adoption of technology is much, much higher than in Europe. If you want a payment from the customers, it is much easier, much faster. That is why you can get high and sustained revenue very early.

R.S.: Can you share a little bit also about your personal experience in helping startups? As a part of CYBERSEC HUB acceleration for Polish startups, you have helped Voicepin. You checked whether they are ready, if they are able and willing to enter Asian markets. What were the biggest obstacles they faced? On the other hand, what was the most competitive part of a European company like Voicepin in entering Asian markets? In your opinion, what are the main opportunities and challenges for companies from Central and Eastern Europe who want to go to Asia?

M.S.: This is probably very similar to what I said before. The chance and challenge is scale. The number one thing is that you can achieve huge scale, so the challenge and, at the same time, the opportunity is tremendous. Do you have the resources to achieve the scale?

Second thing, it is very important to understand the market. It is very true for most Asian markets, perhaps not on the Hong Kong scene, but in countries such as China, Korea, and Japan. They are very different, very unique, each one is different, and to enter these, you need to have someone on the ground. You need to partner with someone who has knowledge of the market, and who is well-connected on the market. I do not know of any startup from outside of this region that would have succeeded without having anyone on the ground. It doesn't have to be your employee, but has to be someone who has lived in Asia, has been there for a long time, has a lot of connections, can open the door for you. Especially in countries like Japan, Korea, China.

Generally, the more the accelerator is focused on one stream, the better for everyone.

R.S.: You now work also with accelerators in the APAC region – Asia and Pacific – what are the main differences from the point of view of an investor who is considering using an accelerator? What are the main differences between the acceleration programs that you can see there and acceleration programs that you can see in Europe, even in Poland?

M.S.: Well, there are differences based on which country the accelerator is based in and who is running the accelerator. And what is the main focus of the accelerator. I am now in four accelerators: two in Hong Kong, one in Taiwan, one in Malaysia. Two of them are government-sponsored, two of them are private. Plus, two of them have a wide scope, they have an "any startup" approach, and two of them are more specific, FinTech accelerators. Generally, the more the accelerator is focused on one stream, the better for everyone: also for investors such as VCs, because they are usually looking for a very particular thing. They are probably not here to see fifty different startups from areas that do not tell them much. It is also easier for the startups, because the accelerator has expertise in this field, it can provide connections and mentoring. And the geography is also important. Why would you join a startup in the Asia-Pacific Region? One, because you want to expand to these new markets, and the accelerator can actually help you with that. The second thing is the question of regulatory environment. If you are in an accelerator in Malaysia, you want to use this accelerator to help you understand the legal issues that you may face entering the Malaysian market. But, for example, when you are in Hong Kong, the legal issues are not that important, so the accelerator really focuses on the commercial side: how they can connect you to the VCs, the funds and customers, and how can they make 'in-roads' into the market in commercial terms.

R.S.: Thank you for all the information. I do believe it may be useful even for the startups that we have seen on the stage during our pitch deck contest, because in the end it is not only San Francisco, Berlin or London. Nowadays it's also Beijing, Schenzen and other Asian destinations, towards which they want to expand. Thank you very much.

M.S.: Thank you very much. ■

THE CANADIAN INSTITUTE FOR CYBERSECURITY

PROTECTING GLOBAL CITIZENS IN THE CONNECTED COMMUNITY

The worldwide cybersecurity and cyber analytics market is facing unprecedented growth, with market size estimated to reach $170 billion in two short years. The size of the growing market is in direct correlation with the rising global cost of cyber-attacks, an expense expected to grow to $2.1 trillion by 2020. Cybersecurity and privacy, once issues only for technology experts, have become widespread concerns in both the business sector and for the general population. Cybersecurity is no longer just Brunswick has played an integral role in cybersecurity research and innovation in Canada.

Today, the University has the largest network security research group in the country, and is well positioned to lead this effort through the Canadian Institute for Cybersecurity (the Institute). The Institute, housed at the University of New Brunswick, is working with industry, the federal government, and provincial governments to solidify Canada's position as a world-class cybersecurity hub for innovation and talent development. Our vision is to become one of the leading training and research institutes in Canada by 2021 by conducting cutting-edge research in cybersecurity.

Source: Rob Blanchard Photo UNB

The team behind innovative ideas and ground-breaking research into the most pressing cybersecurity challenges of our time.

UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK | Canadian Institute for Cybersecurity

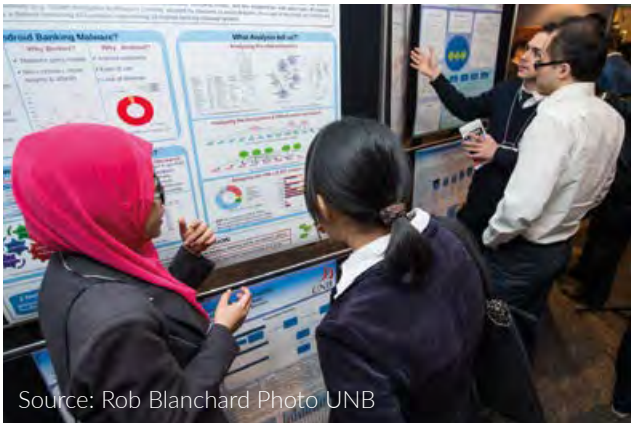
Closing the Skills Shortage Gap

Training and education in cybersecurity are falling short of current, and even future, needs. The present cybersecurity skills shortage in Canada leaves the public, private sectors, and governments vulnerable to attack. The science of cybersecurity is about managing risks and avoiding surprises. At the Institute, we view cybersecurity as a practical problem requiring practical solutions. For the last two decades, our institution has drawn upon multimillion dollar, industry-sponsored R&D in network and systems security to build cybersecurity solutions to protect cyberspace. We are a catalyst for creating an efficient cost-sharing mechanism through which educators, researchers and practitioners can work together with the private sector to advance cybersecurity knowledge and capabilities.

The science of cybersecurity is about managing risks and avoiding surprises. At the Institute, we view cybersecurity as a practical problem requiring practical solutions.

We have a team of nearly 50 researchers, technical staff, and graduate students using state-of-the art infrastructure – we are bringing together researchers from across the academic spectrum to share innovative ideas and carry out ground-breaking research into the most pressing cybersecurity challenges of our time. The Institute focuses on comprehensive multidisciplinary training, research and development, and entreprurial activities that draw on the expertise of researchers in science, business, computer science, engineering, education, law, and the social sciences.

Our research has even spurred the establishment of several spin-off companies. The University of New Brunswick was among the first to recognise cybersecurity as an industry, and prompted the creation of Q1 Labs in 2000, which was acquired by IBM in 2011.



2016 Computer Science Research Expo

Addressing the Threat of Malicious Insider and Outsider Activity

A customer-centric digital model has led to high consumer expectations in both digital experience and data security and privacy protection. Users expect an exceptional digital experience delivered through numerous real-time, digital channels on a 24/7 basis with trusted security protection. According to an IBM XForce report, the worldwide financial sector was attacked more often in 2016 than at any other time in history, and over 50% of the attacks were due to insiders, mostly human error, such as phishing attacks[1].According to the National Fraud Survey, in the United States alone internal attacks cost approximately $400 billion per year, of which $348 billion can be tied directly to users[2]. It is for this reason that monitoring and managing users' actions is paramount for cybersecurity and compliance reporting.

The Canadian Institute for Cybersecurity is currently developing a people-centric cybersecurity solution to address malicious insider and outsider activities. Legislation and regulatory policy are emerging cyber crime. The framing of cybersecurity in legislation and policy may prove a significant influence on how companies approach cybersecurity threats.

The Canadian Institute for Cybersecurity is currently developing a people-centric cybersecurity solution to address malicious insider and outsider activities.

It is important to appreciate that financial institutions are also facing a growing number of security compliance issues, mandates, standards, and regulations in addition to cyberprotection policies. As a result, they encounter multiple overlapping issues, which result in increasing costs and complexity.

Today, a new technology in the financial services, which combines cloud services with Artificial Intelligence, introduces new risks and thus requires new approaches.

The Origin of the Cybersecurity Ecosystem in New Brunswick: A Hotbed of Innovation

Cybersecurity today, compared to late 1990s, has undergone a drastic change. The progress made along the way is rooted in the recognition, early in the Internet era, that the Web was going to be exploited in much the same way as offline business. The explosion of life-altering technology and the ubiquity of the Internet have made it easier for hackers and much harder for businesses and individuals to stay 'safe'.

In January 2001, Q1 Labs founders Chris Newton, Sandy Bird, and Dwight Spencer spun off, from The University of New Brunswick (UNB), their anomaly detection software capable of monitoring large amounts of network transactions and detecting unusual spikes in traffic. "This was right after the Internet boom and there were a lot of worms and viruses wreaking havoc on the university's Labs and former CTO of IBM Security. "We built a technology to detect anomalies in network traffic." This ground-breaking big data monitoring technology, then called Q1 Labs QVision, is today at the core of IBM Security QRadar Software.

[1] http://branden.biz/wp-content/uploads/2017/06/IBM-X-Force-Threat-Intelligence-Index-20.pdf

[2] www.csoonline.com/article/2120631/access-control/the-enemy-inside.html

Ali Ghorbani, Director (CIC) & Canada Research Chair in Cybersecurity

The Cybersecurity Hub at the University of New Brunswick is one of only eight universities in North America chosen by IBM to help in its fight against cyber-attacks. Our computer science students, led by Ali Ghorbani, Director of the Canadian Institute for Cybersecurity, former Dean of Computer Science, and Canada Research Chair in Cybersecurity, are helping IBM's Watson to process and analyse massive amounts of cybersecurity data.

The explosion of life-altering technology and the ubiquity of the Internet have made it easier for hackers and much harder for businesses and individuals to stay 'safe'.

IBM is an R&D partner of the Canadian Institute for Cybersecurity, continuing in the footsteps of the Q1 Lab tech founders, supporting further research and development of QRadar's capabilities.

The Information Security Centre of Excellence (ISCX) at the University of New Brunswick has played an important role in the success of new technology companies, like Q1 Labs as noted above. ISCX also spun off Sentrant Security Inc. in 2012 and Eyesover in 2014. Eyesover provides an online media monitoring and issues discovery solution for customers including political parties, utilities, public and private sector corporations, and governments. The system is the product of research from the Intelligent and Adaptive Systems (IAS) Research Group within the Faculty of Computer Science at the University of New Brunswick, led by Dr. Ali Ghorbani.

Aiming to transform its economic landscape toward a knowledge-based economy, New Brunswick is strategically focusing on technological innovation in cybersecurity. Local government agencies, namely Opportunities New Brunswick and CyberNB, are currently working with industry, other government agencies, and universities to establish New Brunswick's leadership in Canada as a world-class cybersecurity hub. The University of New Brunswick has by far the largest network security research group in Canada and is well poised to lead this effort.

The New Brunswick Cybersecurity ecosystem includes new companies, such as: dGrief, Beauceron Security Inc., EhEye Inc., Sentrant and EyesOver, BulletProof, F6Networks, and BlueSpurs. Bell Canada recently joined the New Brunswick cybersecurity hub as a member of the Canadian Institute for Cybersecurity, and future announcements are anticipated. ■

A History of Technological Innovation:

New Brunswick has been actively supporting information and communication technologies (ICT) as a growth sector. Recent acquisitions of hyper-growth New Brunswick companies like Radian6 and Q1 Labs by industry giants Salesforce and IBM, respectively, have captured national attention and put New Brunswick on the map as a testbed for technological innovation. The total amount of these two transactions is believed to be nearly $1 billion.


CYBERSEC
EUROPEAN
CYBERSECURITY FORUM
Kraków
8-9.
10.
2018
THE QUEST
FOR CYBER TRUST
STATE
STREAM
DEFENCE
STREAM
FUTURE
STREAM
BUSINESS
STREAM

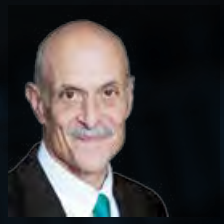
CYBERSEC 2017 - SELECTED SPEAKERS

During CYBERSEC 2017 more than 150 panelists were Dealing with Cyber Disruption. The takeaways and recommendations were inspired and crafted by many of them, including:

Beata Szydło
Prime Minister
of Poland

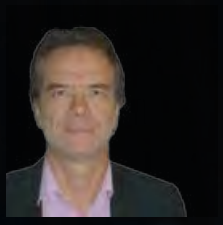
Sir Julian King
European
Commissioner
of the Security Union

Anna Streżyńska
Minister of Digital
Affairs - Poland

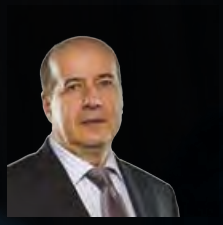


Michael Chertoff
Co-founder and
Executive Chairman
of the Chertoff Group,
Former U.S. Secretary
of Homeland Security

Janis Sarts
Director of the NATO
StratCom Centre
of Excellence



Alexander Seger
Executive Secretary
of Cybercrime Con-
vention Committee
and Head
of Cybercrime Division
at Council of Europe



Ambassador
Sorin Ducaru
Assistant NATO
Secretary General
for Emerging Security
Challenges

Christian-Marc
Liflander
Head of the NATO
Cyber Defence
Section

Marietje Schaake
Member of the
European Parliament,
Founder and Member
of the European Parlia
ment Digital Agenda
Intergroup

Jakub Boratyński
Head of the Trust
and Security Unit
at the European
Commission

Ambassador
Marina Kaljurand
Chair of the Global
Commission on the
Stability of Cyberspace

Luigi Rebuffi
Secretary General
of ECSO

Johan Arts
Vice President at IBM
Security Europe

Alastair Teare
Chief Executive
Officer at Deloitte
in Central Europe

Jan Neutze
Director of Cybersecu-
rity Policy at Microsoft
EMEA

THE HAGUE SECURITY DELTA:

THE DUTCH METHOD OF COLLABORATION AND INNOVATION FOR SECURITY

BY RICHARD FRANKEN

The Hague Security Delta (HSD) is a leading security cluster in Europe. In this Dutch cluster, businesses, governments, and knowledge institutions work together on innovations and knowledge in the fields of cybersecurity, national and urban security, protection of critical infrastructure, and forensics.
They share a common goal: more business activity, more jobs and a more secure world. This article describes how we are realising this goal in the Netherlands.

Over 270 organisations, including governments, businesses and knowledge institutes, participate in the Dutch national security cluster known as The Hague Security Delta (HSD). They engage within HSD to meet other participants and explore potential opportunities for further collaboration. The HSD innovation liaison team works closely with investment companies and the Dutch Chamber of Commerce in order to connect national as well as international businesses to the HSD security cluster.

Programming Innovation Projects

The HSD organisation, with the HSD Office as its operational arm, functions as an independent platform that aims to promote ongoing and effective collaboration and interaction between government bodies, businesses, and knowledge institutes. It accelerates and supports the so-called triple helix form of collaboration in a variety of ways. The HSD Office can be viewed as the 'oil' that ignites, lubricates, and maintains this triple helix collaboration 'engine' in good order.

As such, it serves as an interface that connects the supply with the demand side, i.e. parties searching for suppliers with potential providers of knowledge, innovation, market opportunities, financing, and talent development.

HSD provides an open and trusted environment in which the new forms of collaboration, business models and innovation that are needed to produce security solutions can actually be developed and put into practice. HSD is based on a growth model facilitating the development of an increasingly close-knit network of partners, a network based on mutual trust and focused on knowledge and ongoing innovation within a national as well as international framework. In this network, different actors with relevant expertise and experience continually take turns in taking the initiative to develop new and innovative solutions as an agent or connecting factor. In this manner, the HSD Office is able to fill four important roles when it comes to programming innovative projects in the area of security.

1. Setting the agenda and creating opportunities for further action

HSD initiates sophisticated exploratory investigations into security-related topics with an eye to the future. These studies aim to provide a shared and consistent framework for the triple helix partners to collaborate on practical solutions in the security domain. This can serve to promote and raise the profile of existing ideas and initiatives, or get them on the agenda in the form of new initiatives or activities[1] . HSD also creates additional opportunities for collaboration, for example by creating environments for testing practical solutions and/or formulating relevant guidelines and regulations.

2. Connecting

HSD makes it easier to connect different stakeholders, providing physical as well as virtual meeting places. It organises events dealing with specific topics and themes, so that relevant target groups and associated contacts can raise their profile and communicate their message.

HSD is also actively involved in 'matchmaking'. With a helicopter view of the parties participating in the HSD network, the HSD Office is very well positioned to connect relevant players with each other or with ongoing or new collaborative initiatives. HSD also initiates learning and talent development programmes to train the specialists and decision-makers of the future, and to introduce young talents to interesting work environments and potential employers.

3. Facilitating

HSD also plays an important role as a central repository for acquired knowledge and lessons learned. For example, HSD carries out studies into the factors that determine success or failure of collaborative projects and processes. The results of these studies and the associated track records are registered over time in the form of checklists, methods, 'how to' folders etc. Practical examples from the past are then used to create and shape new successful initiatives.

[1] *Strategie Nationale Veiligheid - bevindingenrapportage* (Den Haag: NCTV, 2013).

HSD also maintains an ongoing and growing registry of relevant procedures, innovation and acquisition agendas, and financial instruments. It functions not only as an accessible and expert helpdesk in such matters, but also as a connection point for parties looking for suppliers and relevant providers, drawing their attention to potential opportunities for collaboration and innovation. One of the ways HSD does so is by publishing a financing index with an overview of relevant funds, subsidies, business-to-business funding and other funding sources offered by the government, external knowledge programmes and private investors. In addition to Dutch funding sources, HSD also identifies and communicates European and international opportunities such as the Horizon2020 fund for innovation from the European Commission and the UNIIQ investment fund aimed at accelerating the introduction of innovations to the market. Finally, the HSD Campus, which was developed specifically for that purpose, functions as a meeting place for partners wishing to engage in meaningful collaboration.

4. Mediating

The HSD Office, or a different neutral party, can serve as an impartial mediator offering consultations between different parties. This type of independent and expert role can, for example, also be useful when an evaluation is needed or when an 'arm's-length' management is needed, with a focus on substantive or process-related matters.

Delivering Added Value

The roles played by HSD, as described above, enable it to deliver added value in the following forms:

Access to Knowledge

HSD's increased insight into relevant security issues is critical. It furthers the ongoing triple helix collaboration, enabling the participants to share knowledge and learn from each other's experience. HSD identifies, collects and explores knowledge requirements, outsources research, and publishes reports and issue briefs. In addition, HSD brings parties together to discuss current themes, for example during the international Cyber Security Week in The Hague.

Access to Market

From the perspective of the supply and demand, partners are looking to collaborate on projects that lead to the development of shared innovative solutions for complex security challenges facing modern-day society. It is therefore logical to conclude that the ability to match supply to demand, and subsequently connect the relevant players is critical to the success of an open and innovative framework.

Access to Capital

There is a need for financing and capital in all phases of innovation and development. HSD provides access to relevant sources of funding in order to streamline access to various forms of financing in the different phases of innovation based on the content at hand. Such requirements are especially evident in the SME and start-up sector. The HSD Office serves as an interface between the supply and demand side with regard to financing and capital.

Access to Talent

There is a great demand for well-trained employees on the part of public as well as private partners. HSD has developed a Human Capital Agenda that aims to ensure a better fit between the educational system and the business community and a better alignment with the rapid pace of new developments via greater collaboration between participating partners and educational institutions.

Access to Innovation

HSD provides an open innovation framework within which public and private parties can work together pre-competitively to develop new ideas, services, and products. This type of partnership lays the foundations for new forms of cooperation and consortiums between the participants.

Leverage the Power of Collaboration

Collaboration between governments, businesses, and knowledge institutions – in other words the triple helix collaboration – is the key to HSD's position as the leading security cluster in Europe.

This type of collaboration is crucial for innovations in the security domain and delivers added value to all parties concerned[2].

The triple helix collaboration is an ideal opportunity for public sector actors to carry out the tasks delegated to them by the society more efficiently and effectively. By collaborating with the private sector, they can obtain access to additional knowledge, resources, network contacts, and communication channels, as well as new innovations and technological developments. This can result in a broader base of public support, financial benefits and/or improved results as well as increase their effectiveness in achieving social change[3].

Via the triple helix collaboration, private parties can actually implement their corporate social responsibility policies and raise their profile and positioning in the market. Participation can also provide them with opportunities to market (security-related) products or services more easily and quickly and to help innovate their business processes. The triple helix collaboration also allows them to experiment with creative solutions, develop new products or services, and reach new markets or target groups for their products or services. The overarching goal of private parties here is to ensure the sustainability of their business.

The triple helix collaboration is an ideal opportunity for public sector actors to carry out the tasks delegated to them by the society more efficiently and effectively.

Knowledge institutions are an important third player in the triple helix collaboration. For example, as knowledge partners, they carry out research into issues for which solutions are required within the framework of the triple helix collaboration. On that basis, they can identify the 'problem behind the problem' and help conceptualise and develop innovative solutions or approaches. These institutions validate the final results until there is no doubt that the triple helix collaboration has developed a successful solution for the problem at hand. Accordingly, the triple helix collaboration always leads to new knowledge becoming more widespread and available.

Together, the three parties mentioned above have access to an enormous pool of knowledge, capital, and innovative capacity that can be utilised for the benefit of a safer and more secure society. Thanks to the ongoing triple helix collaboration within HSD, they can share and leverage each other's strengths to develop new policies or guidelines as well as new products and services.

More Value for Money

Different cultural backgrounds of parties collaborating within the triple helix framework create opportunities for leveraging their strengths. By working together, participants realise their own organisational objectives as well as shared aims and social goals. A successful triple helix form of collaboration creates a win-win-win situation for all the parties involved[4] . However, several preconditions are important to realising these goals, which are encapsulated in the acronym STER: - Shared interest - Trust - Equality - Results.

Based on the above STER parameters, the triple helix partners contribute to realising the collective mission, goals, and tasks. The parties involved respect their own differing positions in the society and appreciate each other's unique characteristics. This point of departure makes it possible for them to work together as equals to achieve better results, and to deliver greater 'value for money' than they would as individual players. The synergy within the triple helix alliance means that the whole is greater than the sum of its parts.

Their aim is not to maximise their own interests at the cost of the other, but rather to align the interests and actions of the individual parties. Credibility and integrity are important building blocks underpinning the collaboration.

[2] Richard Sennett, Together: *The Rituals, Pleasures and Politics Of Cooperation* (Yale University Press, 2012).

[3] *iOverheid* (Den Haag, Wetenschappelijke Raad voor het Regeringsbeleid, 2011).

[4] Erik-Hans Klijn en Mark van Twist, Publiek private samenwerking in Nederland (Tijdschrift voor Management & Organisatie, nr 3/4, 156-170).

Table 1: Characteristics of a triple helix. Source: The Hague Security Delta

Triple helix characteristics	Possible implications for the organisation
Triple helix collaboration is one of the instruments that parties can utilise to realise their individual organisational goals.	It is a strategic activity within the organisation, and the organisation will have to make a well-considered choice as to where and when this instrument will be utilised.
There is a lack of hierarchy between the collaborating partners.	This requires specific agreements and mechanisms of coordination, the willingness of the parties involved to give up total control of the process and results, and coordination between the parties regarding the aspects over which they wish to retain control.
Collaboration between parties which can differ in terms of their mission, goals and interests, funding, manner of working, and culture.	These differences are actually a source of strength (complementarity, heterogeneity ...), but differences can also lead to disruption and conflict. This requires adequate attention on the part of the management with a focus on preventing, reducing, and/or lessen potential friction points.
The parties continue to operate autonomously and work together on a voluntary basis, and the collaborative framework is of a temporary nature.	This means that there is always an inherent tension built into the collaborative framework between cooperation aimed at realising shared goals on the one hand and competition aimed at realising individual interests on the other. The fact that the collaboration is of a temporary nature means that agreements are needed about the duration and possible premature termination of the collaboration, an explicit definition of individual goals and what the collaboration must, as a minimum, deliver in terms of results to ensure that the organisations involved continue to invest in it or even increase their investment, and how and under which circumstances the collaboration can be ended.
Parties depend upon each other in order to realise their individual and shared goals.	This means that it must be clear what the unique added value contributed by each party is, what the shared goal is, and which resources each party will contribute and when and under which conditions they will do so. Adequate attention must also be given to potential abuse of power, a possible lack of synchronicity between the individual resources contributed and the realisation of individual benefits desired, and free-riding.

Mutual trust is a key element of such an alliance. Differences between parties are discussed and resolved in an open and transparent atmosphere. The parties communicate with each other openly and directly, and are willing to give each other insight into their individual qualities and capabilities. Individual and shared interests are identified and communicated, and the parties are happy to see other members of the alliance succeed. Their aim is not to maximise their own interests at the cost of the other, but rather to align the interests and actions of the individual parties. Credibility and integrity are important building blocks underpinning the collaboration.

Choose the Right Partner

As explained earlier in this chapter, the triple helix collaboration is a logical choice and an effective framework for structuring mutual collaboration between the government sector, the private sector, and the knowledge sector. Such collaboration results in 'useful participation' in the words of Maurits Sanders, a lecturer in Governance and the Executive Director of the Netherlands Institute of Government[5]. In order to actually make this useful participation happen, it is important to ensure that the triple helix alliance is structured with the concept of network management in mind. The parties must collaborate as equals and link their networks to one another. The structure is not hierarchical, and the parties are connected to one another for a longer period of time, as opposed to a general project management type of framework that often involves a brief and sometimes superficial form of collaboration.

Differences or points of friction between parties are resolved through mutual consultation, and the goal is to achieve high-quality and beneficial results in the medium to long term. Based on a shared vision, the parties succeed in integrating their individual organisational goals and formulating a shared goal in a manner that allows them to connect on the basis of mutual interdependence and trust.

According to Eversdijk and Korsten[6], by drawing on such network-orientated concepts, the parties should identify each other and structure their triple helix collaboration as early on as possible. It is not advisable to first structure the collaborative venture and only then start searching for partners.

Vos and Tjemkes argue that a great deal of thought and energy should be invested in the selection of partners. They warn against simply approaching the best-known parties or parties located in the same network via mutual relations. This often leads to lengthy negotiations about the goals of the collaboration that the partners wish to realise together and the conditions under which this should occur. As a result of such efforts, partners who deliver only limited added value still continue to participate in the collaborative framework, which in turn disrupts the collaborative process. The only advantage of such an approach is that relatively little effort is required to select the partners. Vos and Tjemkes opt for a more systematic approach whereby an organisation carries out a targeted search for partners who deliver added value and offer a good fit with one's own organisation. The advantage of this approach is that each partner really makes a contribution to the predefined organisational goals. The end result is greater commitment of the partners, mutual synergy, and a shared ambition to realise a collective goal.

In the case of the triple helix collaboration with several partners, it is a good idea to pay extra attention to:

– the relationships between the parties concerned: are they competitors? What is the balance of power between them?
– the composition/distribution of the partners: what is the public/private ratio? Do the individual contributions and benefits balance one another?
– the added value provided: what is the interest of each party to collaborate? What is each party's unique contribution?
– pre-existing relationships: to what extent will the triple helix collaboration affect other possible

[5] Maurits Sanders, Publiek-private samenwerking, een reparatiestrategie voor falende ordeningsvormen (University of Twente, Public Administration, 2014, 67-76).

[6] Arno Eversdijk en Arno Korsten, *De bestuurskundige mythe van verbindend PPS-management* (Bestuurswetenschappen 3, 2008, 29-56).

cooperative relationships with these partners in their own organisations?

Ensure Effective Process Management

When it comes to collaboration within a triple helix alliance, a great deal of attention is often paid to financial matters and the collaborative structure, but almost no attention is generally given to the management of triple helix processes. Collaborative agreements are entered into without proper preparation in terms of the basic points of departure, organisational structure, management and processes. This would not have to be such a problem if process management was not all that important. However, empirical research carried out by Klijn and Van Twist makes it clear that (interaction) processes do play a very important role.

As a rule, the triple helix collaboration involves a lengthy and complex path to realising the desired results. Achieving a satisfactory conclusion is far from simple and demands a great deal of management effort[7]. Accordingly, extra attention needs to be given in the future, especially by government players and policy makers, to the role of managers in the triple helix alliance, and in particular to the difficult choices faced by managers in their daily project activities. This is where a real potential for improvement exists and where opportunities are present for an accelerated, broadened, and improved realisation of the projects involved.

A manager in a triple helix alliance needs to ensure that decisions are taken on the basis of consensus. Each party must agree, as each party has an interest in ensuring that the collaborative venture realises its goals. The vote and interests of each party count. Exerting pressure to force through a decision puts a strain on the collaboration and makes it difficult to achieve the best possible result. A manager, therefore, needs to know how to best ensure that decisions within an organisation are taken appropriately and harmoniously. The manager also needs to have an understanding of change processes. After all, the triple helix collaboration is all about change and innovation aimed at resolving issues that are important to society. In addition, the triple helix collaboration, in and of itself, often involves a process of transformation, as the collaboration also has an effect on the participating organisations. This can lead to internal resistance within the individual organisations, and the manager must be able to deal with such issues effectively.

A triple helix manager must stand 'above the parties'. He or she must be independent and at the same time be able to bring the parties together. The manager must speak the language of all the parties concerned and be able to relate effectively to different cultures. He or she must be result-focused, decisive, sensitive to political and administrative considerations, and have the appropriate networking skills. The manager must also be aware that in everyday life decisions are generally affected by a host of factors, including emotions, subjective preferences, past experiences, personal perceptions and meaning. The focus within triple helix alliances is often on commercial aspects whereas the (un)conscious 'decision' to trust another party is based on a very different set of factors. A manager must therefore be able to 'play with' a broad palette of factors that contribute to the success of the triple helix collaboration. He or she must be able to act as a bridge between different parties and have insight into group processes and the human side of collaboration.

A manager in a triple helix alliance needs to ensure that decisions are taken on the basis of consensus.

Of course, the commercial aspects of the triple helix collaboration are also important, as the ultimate goal of the parties is to realise the collective as well as the individual and organisational goals. A business case is a useful tool to identify and describe the benefits that the triple helix collaboration can ultimately deliver to the parties concerned. Companies are used to formulating their own financial business cases in pursuit of the above, but government bodies often find it difficult to come up with the same kind of arguments. However, they can do so if they think

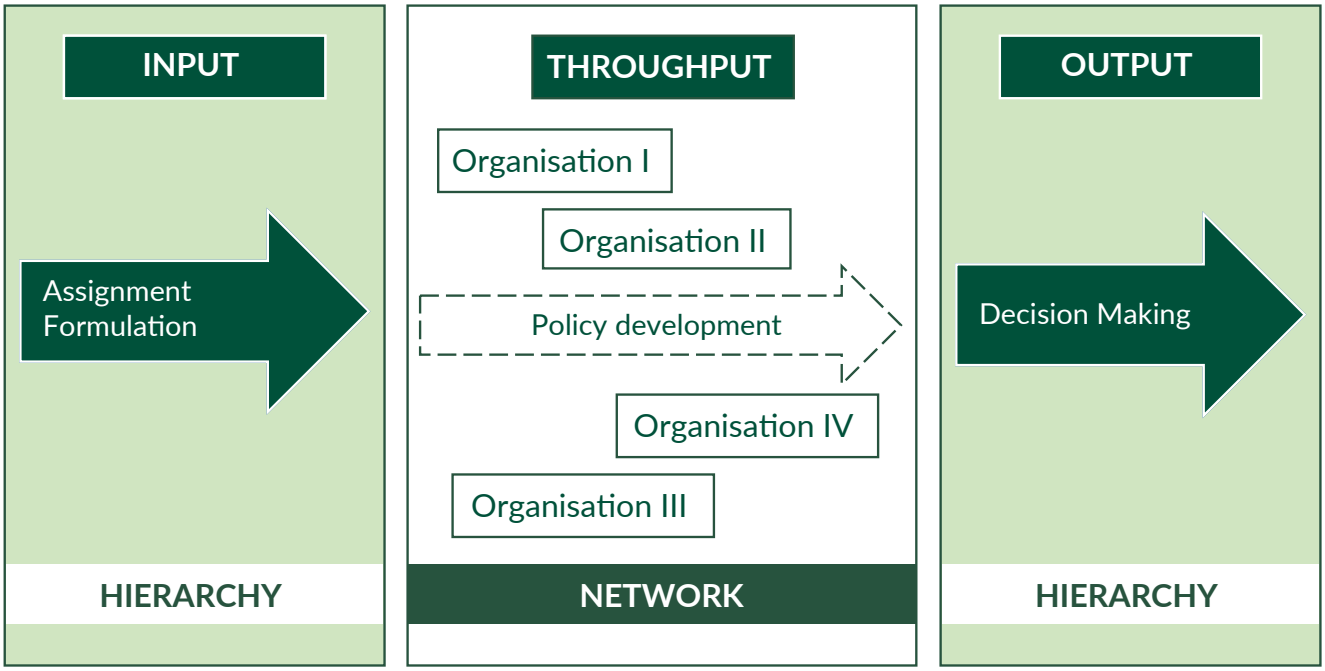
[7] Mark van Twist, Erik-Hans Klijn, Jurian Edelenbos en Michiel Kort, *De praktijk van publiek-private samenwerking, hoe managers omgaan met complexe PPS-projecten* (Tijdschrift voor Management & Organisatie, nr 6, 2006, 24-43).

more in terms of social benefits or the 'public good'. Benefits to society result from identifying the connection between the social problem in question on the one hand and the desired result and effect on the other, while at the same time specifying the costs of the collaboration and the resulting benefits, financial or otherwise, to society.

Governance

Governance has long been synonymous with management and guidance by government. However, due to changes in society, governance and the public norms and values associated with governance are increasingly defined in collaboration between government bodies, the business sector, knowledge institutions, social (action) organisations, and citizens. The public domains becoming the playing field for a great many different parties and the institutional field is becoming ever larger, busier, and less transparent. Whereas governance was traditionally based on hierarchical lines set out by government bodies, we have seen the rise of a more 'networked' society in which new and ever-changing networks of players cooperate, depending upon the specific social problem at hand. Maurits Sanders also addresses this change[8]. He argues that the formulation of policy has increasingly become a matter of collaboration between government entities and private partners. Due to the nature of government as a public body, with important governance principles such as openness,

Figure 1: Legitimacy and the decision-making process in a triple helix collaboration[9]



[8] Maurits Sanders, *Legitieme besluitvorming door PPS* (Recht der Werkelijkheid 2010 (31)1, 80-84).

[9] Maurits Sanders, 'Recht der Werkelijkheid 2010 (31)1 – Werk in Uitvoering, Legitieme besluitvorming door PPS' (Reality rules 2010 (31) – Work in Progress, Legitimate decision-making by PPS).

integrity, efficiency, legitimacy, and accountability, the multiple roles of government built into a triple helix alliance raises questions of legitimacy. Sanders: "In the decision-making process, policy is formulated outside the hierarchical framework of authority and institutionalised bureaucratic frameworks. This happens because the government is dependent upon the cooperation and input of expertise on the part of other organisations for the realisation of collaborative projects. Accordingly, policy-related activities take place not only within the civil service organisation but within the sphere of influence of different organisations that are part of the (policy) network."

This issue of legitimacy does not necessarily pose an obstacle to entering into the triple helix collaboration. Policy and/or solutions to social problems may then be formulated within the network, but when they are returned to the governmental hierarchy for the definitive decision-making process, there are appropriate safeguards in place with regard to legitimacy and governance. Ideally, the formulation of the request to form a triple helix type of collaboration also takes place within the hierarchy of government. In process terms, we then speak of hierarchical input and output, whereas the throughput takes place inside the network. This manner of working is quite feasible within a triple helix alliance, as each public and private party has and retains its own specific responsibilities and authorities. In other words, from the perspective of governance, there are no real obstacles to establishing a triple helix form of collaboration. ■

This article is based on Pepijn Vos and Frederik de Vries' publication, "Boosting your triple helix cooperation" (The Hague, HSD, 2016) and on Ida Haisma's publication "Publiek-private samenwerking: kicken of killing? (Grip op Crisis, 2016, 77-114). The author would like to thank Martin Bobeldijk for his contribution.

ABOUT THE AUTHOR:

RICHARD FRANKEN

"Security is now more than ever a top priority in our society. In this changing society we need to look at other ways than the traditional approach in order to create results. Effective innovation calls for cooperation between disciplines." For this reason, Richard became one of the founding fathers of The Hague Security Delta. Richard started his career in the security domain at the National Police Corps, where he held different positions and from which he transferred into the private security sector. Before becoming Executive Director at The Hague Security Delta, he worked in a dual employment as Commercial director for Trigion and as Executive Director for Hoffman Bedrijfsrecherche, a business focused on digital investigations and cyber security. Richard was also active as a board member of the Dutch security industry association' and of 'Coess' (the international Security sector industry association), was a staff teacher risk management and commissioner & advisor of several organisations in the sector.

CYBERUSLABS

FROM SILICON VALLEY TO POLAND

Cyberus Labs, Sp.z.o.o. is a new kind of Polish company that is global in its DNA. Co-founded by Silicon Valley and Polish entrepreneurs, Krakow-based Cyberus Labs is cyber-security startup that is introducing innovative cybersec products to the Polish and European markets. At Cyberus Labs we have chosen not to "patch a leaking ship" but to bring a new approach to some vexing security problems.

Founded by George Slawek (CEO), Jack Wolosewicz (CTO) and Marek Ostafil (COO), the company has right from the beginning set its own course - to focus on eliminating cyber threats, and to deliver solutions that will be both secure and easy to use.

PASSWORDS ARE A BROKEN SYSTEM

The use of passwords is a broken system. This has been known for many years, however, we have struggled to find a good alternative to this ubiquitous user authentication system. Companies are vulnerable to data theft of credentials while users struggle to create, remember and input dozens of username/password combinations just to manage daily online life.

To date, alternative user authentication methods such as biometrics have had limited success in the market place for two key reasons, 1. privacy/security concerns (e.g. theft of user biometric data) and 2. poor user experience.

The reality is that the username/password login method is still by far the most popular user authentication method. As a result hackers or other bad actors continue to find ways to steal user credentials through ever more sophisticated data breaches. It is estimated that over the last 5 years approximately 1.5 Billion sets of user credentials have been stolen, almost half a billion alone from the 2014 Yahoo data breach announced 2 years later in September 2016.

As Michael Chertoff, former head of US Homeland Security, recently stated, "A closer examination of major breaches reveals a common theme: In every "major headline" breach, the attack vector has been the common password. The reason is simple: **The password is by far the weakest link in cyber-security today**."

A DIFFERENT APPROACH

Cyberus Labs has taken a different approach to finding a solution to the user authentication challenge and dilemma – the right balance between the need of the user to have a fast and convenient way to log into their online account and the need of the company to have a secure and effective user authentication system. **At its core is the elimination of the username/password combination as a user authentication methodology**.

The result of our 3 years of research and development in Silicon Valley, CA and in Poland is the CYBERUS KEY password-less logon platform, formerly launched in September 2016 at the Kosciuszko Institute's CyberSec 2016 conference in Krakow, Poland.

CYBERUS KEY is password-less logon and authorization platform that the user accesses their online account by activating the Cyberus Key mobile application on their smartphone and with one-click logs into their banking or e-commerce account on their laptop.

The user is authenticated without any username/password or any "actionable" data being used or transmitted at the time of logging onto their account. In other words, there is nothing for hackers to steal.

A PASSWORD-LESS WORLD

CYBERUS KEY enables a user to securely logon to any web service (for example: banking, e-commerce, e-health, media platform) using a preinstalled application on a mobile device by securely transmitting an audio signal between the device and the web service via a laptop or another mobile device – authenticating that user's credentials instantly and securely by generating an "unbreakable" short-lived unique onetime password.

The technology of generating and transmitting a one-time-password by the use of the audio signal makes the Cyberus Key system highly secure because:
a) no useful or actionable data for cybercriminals to steal.
b) the characteristics of the audio signal used for user authentication makes it impossible for cybercriminals to compromise.
c) short-lived (few millisecond) one-time password expiration prevents cybercriminals from intercepting or re using.

The benefits are both on the user side and on the operator's website side. The user will no longer need to remember and type in user names and passwords - a tedious, inefficient and inherently insecure method of user authentication.

CYBERUS KEY patent pending technology disintermediates the interaction between users and websites, bypassing User ID/Password requirements currently used for authentication.

CYBERUS KEY creates a truly secure log on experience and verifies both sides of an on-line transaction, eliminating the risk phishing, key-logging, "man-in-the-middle" or "man-in-the-app" types of cyber attack.

CYBERUS KEY gives users fast, single touch and secure access to their on-line accounts. There is no more need of costly FOBs, Tokens, SMS'.

CYBERUS KEY offers additional integrated security measures via multi-factor authentication such as biometrics, for high-value, high-risk transactions. The system is fully customizable to meet the specific needs of financial services, government, e-commerce and many other sectors. CYBERUS KEY is also delivering new marketing/sales channels with highly targeted offers to mobile app users in real-time on a 2nd screen.

CYBERUS KEY can be Cloud/SaaS or client-side "on-premise" installation.

THE FUTURE

Automated systems of connected devices in Internet of Things (IoT) e.g. "smart homes" systems -connection of household appliances, air conditioning, heating, power, light, entertainment etc. is a fast growing market. CYBERUS KEY will offer user-to-machine and machine-to-machine authentication solutions ensuring effective authentication and authorization.

CYBERUS KEY proposes a mechanism which will add IoT device identification, authentication and will govern the types of interactions which can be legally performed by devices and to allow only authorized actions to be undertaken by IoT devices.

KRAKOW

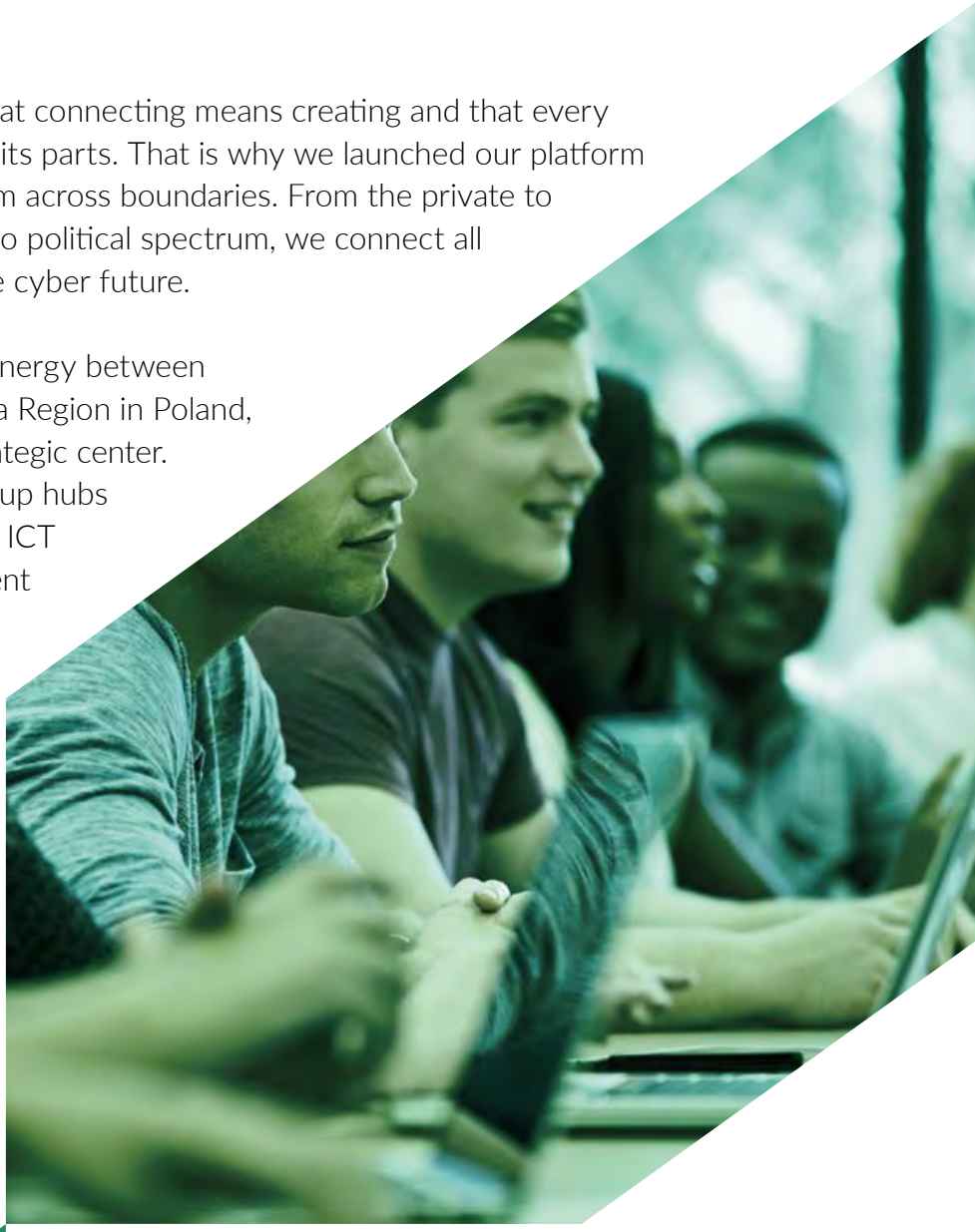
THE PLACE WHERE CYBER MEETS SECURITY

THE KOSCIUSZKO INSTITUTE

WHAT **WE** DO?

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum CYBERSEC, one of the main public policy conferences on cybersecurity.



One of the initial projects run by our platform is CYBERSEC Accelerator which helps ICT and cybersecurity startups and SMEs from Małopolska to reach international markets. In the run-up to the project, an expert panel selected 7 of the most innovative businesses amongst the applicants. The Accelerator has been officially launched during the 2nd European Cybersecurity Forum CYBERSEC 2016. In this Innovation Book you will find unique products and services offered by CYBERSEC Accelerator participants.

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship projects in the field of cybersecurity, among them CYBERSEC HUB and the European Cybersecurity Forum – CYBERSEC.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY MARKET