VOL 2 (2018) ISSUE 3-4

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.

EDITORIAL BOARD

Chief Editor: Robert Siudak
CYBERSEC HUB Project Manager and Research Fellow of the Kosciuszko Institute, Poland

Deputy Editor: Dr Joanna Świątkowska
CYBERSEC Programme Director and Senior Research Fellow of the Kosciuszko Institute, Poland

Executive Editors: Marta Przywała and Barbara Sztokfisz

Designer / DTP: Joanna Kaczor

Proofreading: Paweł Matus

ISSN: 2543-7259

European Cybersecurity Market is a quarterly publication.

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

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

© 2018 The Kosciuszko Institute
All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.

FOREWORD

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

Many of us ask at some point: what, actually, is cybersecurity? It is not information security, nor computer security or network security. The first term is broad, encompassing a wide realm of information processing (including non-digital processing), and the other two are sub-disciplines of computer science, while cyber arises from the intersection of ICT and a number of social phenomena from political science, security studies, economy as well as sociology. Therefore, the multidisciplinary quest for the definition of cyberspace must be driven by more than technological factors alone.

Taking into account the aforementioned multi-layered character of the cyberspace, building a successful product or creating a service for this sector is not only about technology. Cybersecurity businesses have to be businesses in the first place. Even the most advanced technology will not be able to find clients without proper market-fit, timing or marketing. Blogs and books are full of stories about ground-breaking technological novelties that stayed in the labs or on the shelfs. That is why one of our goals in the European Cybersecurity Market is to analyse and foresee business, rather than technological trends.

For that purpose, this ECM issue provides the overview of several trends we have mapped. You will find here an article about the need to engage technicallyoriented students and youngsters in order to fill the cybersecurity labour gap. You will also read about the need to know your user and customer better with profiling techniques. The cyberthreats landscape researched amongst SMEs from Poland, Hungary, Slovakia and the Czech Republic will give you an important insight into the client's needs. In the special section of this double issue, we also present the Digital 3 Seas idea and the potential of the Three Seas region in the context of the rapidly growing ICT market.

Robert Siudak

CONTENTS

FILLING THE CYBERSECURITY SKILL GAP WITH BOTTOM UP INITIATIVES: CASE STUDY OF THE CYBERSEC LEAGUE

BY ROBERT SIUDAK, THE KOSCIUSZKO INSTITUTE

The demand for cybersecurity professionals is growing exponentially, with predictions of up to 6 million workplaces and between 1.5 and 2 million unfilled vacancies globally by 2019[1]. The market is also eager for talents from this sector, with 68% companies acknowledging that they have a high demand for cybersecurity specialists[2]. Institutionalised education on all levels is lagging behind the fast evolving IT security field, which creates a need for other stakeholders to actively engage. On the one hand, businesses are doing their best to train employees internally or to attract potential candidates. On the other, institutions in the administration and third sectors are launching a number of initiatives aiming to raise the level of digital and cyber skills. In Lesser Poland, we created a coalition of stakeholders and launched the CYBERSEC League project, with the goal of attracting youth and university students into cybersecurity professions.

The CYBERSEC League was organized by the Kosciuszko Institute and Krakow Technology Park in cooperation with Krakow University of Technology and AGH University of Science and Technology. The idea is to create a new formula of events for IT-oriented students and young professionals that would influence their career decisions. In order to achieve this, we mixed the standard formats, such as hackathon, capture the flag, escape room or city game, and created 'Play the hack'. Players take part in a 24 hour gamified challenge, during which they have to solve cybersecurity riddles, logical quests or even do physical exercises. Everything is embedded in the main plot and enriched by multiple side quests hidden in the open world. This year's edition took place on 19th–20th May in the Krakow Technology Park. The plot took the participants to the year 2045, where the global corporation Adui Industries has been planning to use their computerised system based on Artificial and Human Intelligence for evil. The participants were warned about Adui Industries' plans by a whistleblower from the resistance movement called the League. And then the game began...

One hundred and twenty participants in 28 teams registered to the event. During the game, they had to face technical tasks involving analysis of the network traffic, decryption of HTTP/HTTPS connections, RSA algorithms, Vernam ciphers and visual cryptography. Apart from the main plot of the game,

[1] UK House of Lords Digital Skills Committee, https://www.parliament.uk/digital-skills-committee; CSO, Cybersecurity job market to suffer severe workforce shortage, 2015, [online] www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015- to-2019-indicate-severe-work-force-shortage.html (access: 12/05/2017).

[2] https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf, s.4.

which focused on ICT related assignments, participants explored an open world with hidden QR Codes, which gave them clues about optional tasks. These additional tasks included a geocaching game, logical riddles, escape room or even workouts with push-ups and squats. The teams collected points for solving both the main assignments and the minor tasks. All participants were also given varied 'asset' cards, like in role-playing-games (RPGs), which they used to disturb the work of rivals, help their own team, win additional time and more. After 24 hours and the final assignment, team Sparrows scored the highest number of points and won the competition. All participants received medals certifying their role in rescuing 2045's humanity from the evil plans of Adui Industries.

The innovative formula for the cybersecurity event that we created is based on five main principles:

1. Gamification – stimulate young people by allowing them to be the players;
2. Plot – tell a story that will create additional value for your audience;
3. Everyone is a winner – show appreciation to all participants and give them 'cool' rewards;
4. Engage before the event – communicate with the audience before the event, start the storytelling, give them introductory tasks and ask them about their preferences;
5. Cooperate with the industry – include experts from cybersecurity companies and let them become mentors and partners for the young participants.

When it comes to participants' experience and satisfaction, according to evaluation forms filled by the players, 100% of them would take part in the event again and 100% would recommend Cybersec League to their friends. On a scale from 1 to 5, almost 90% of respondents rated their experience during the event as 4 or 5. The results clearly show that by mixing the formulas and engaging the participants on different layers created by technology, plot and gamification, we were able to attract young people outside from the sector to cybersecurity. And that is our goal.


CYBERSEC
EUROPEAN
CYBERSECURITY FORUM
DON'T MISS THE 4TH EDITION
SAVE
THE DATE
8–9
OCTOBER
2018
FOLLOW US ON:
#CSEU18
WWW.CYBERSECFORUM.EU

BIOMETRIC PREDICTIVE ANALYTICS

HOW VOICE-BASED BIOMETRIC PREDICTIVE SYSTEMS REDUCE FRAUDS AND INCREASE SALES.

BY ŁUKASZ DYLAG AND JAKUB GAŁKA

Introduction

In modern economics, the consumer profile changes constantly. It is common for the consumer to expect order and execution fulfilment, purchase of goods, and any other transactions to be performed instantly, online, and on demand. This leads to an increase in popularity for remote customer service channels. In the finance, insurance, and telecommunications industry, phone channels are particularly utilized as they gradually employ a wider range of services previously available only at the local branches or outlets of organisations.

Regulations in force since the year 2018, i.e. the General Data Protection Regulation (GDPR) and the Payment Services Directive 2 (PSD2), specify law and organizational frameworks for the use of breakthrough, unknown technologies in various economic sectors, both in public institutions as well as private companies. On the other hand, the increasing threat of cyberterrorism as well as online attacks conducted by hackers and scammers are a serious risk, both for the global economy as well as businesses. Developing efficient security is a significant challenge due to the continuous use of bleeding-edge technology both by security experts as well as scammers. A notable example is the development of attacking methods such as conversion and speech synthesis with the use of deep learning, which may pose a threat to voice-based customer channels.

The increasing threat of cyberterrorism as well as online attacks conducted by hackers and scammers are a serious risk, both for the global economy as well as businesses.

Predictive analytics systems

The vast amount of telephone conversations conducted every day requires a significant involvement of both human and financial resources, especially in the telecommunications, finance, and insurance industries. The typical needs of businesses making significant use of voice communication channels to interact with their clients necessitate the use of tools which fulfil the following three key roles:

- Reduce costs of operations;
- Optimise profits from current activities;
- Have impact on satisfaction of current and new clients.

Currently, all large enterprises make use of data analysis tools to achieve their goals, although most of them do not fully meet the imposed requirements. The Business Intelligence systems currently available on the market mainly allow for back data reporting. They allow to figure out what happened. While they can undoubtedly be very useful, the value of such data often proves to be too low in a constantly changing environment. Analyses provided by qualified analysts prove to be crucial in such situations, as they allow to ascertain why something happened.

Currently, all large enterprises make use of data analysis tools to achieve their goals, although most of them do not fully meet the imposed requirements

Unfortunately, there is a shortage of experts with the specialist knowledge and analytical abilities required to perform such tasks at a level of 140,000-190,000 workers in the United States alone, where such solutions are most popular. There is also a shortage of managers and experts who possess the know-how required to make efficient use of the provided analyses as well as to make effective decisions. The acquired analytical data concerns past events, it is therefore not as valuable as it could be if current events were to also be monitored. However, the most valuable aspect, which would meet the requirements of enterprises, is being able to ascertain what could happen in the future.

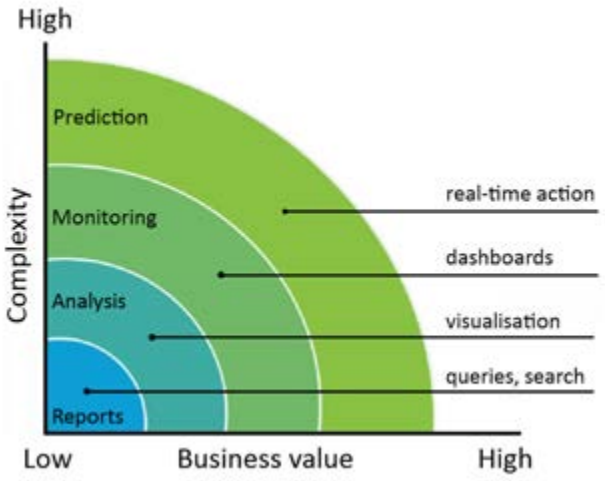


Figure 1. Business value of predictive analytics systems

Voice customer channels

The need of businesses to optimise the marketing, sales, and management processes – in the scope of direct voice communication with consumers via call centre/contact centre (CC), IVR, mobile, and Voice-Over-Web channels – allows these businesses to make use of both archival as well as current voice, text, and transaction data.

Currently, less than 3% of voice data is used for the purposes of analysis and creation of consumer models ("2018 Annual Reference Guide" Report, Speech Technology Magazine, 2018, http://www.speechtechmag.com). This stems from the limitations imposed by the manual or semi-automated methods of data analysis. In the situation where legal and organisational regulations require the maintenance of such resources as well as incurring the costs of such maintenance, and also due to new services emerging in the FinTech industry as part of the constantly developing global market, it is reasonable to make use of such resources in order to generate value, knowledge, and possibilities by way of analysis and the creation of automated prognosis models for the purposes of Business Intelligence. Being able to analyse and meaningfully use 100% of voice resources could allow for the implementation of new solutions in this scope, therefore creating a new market.

The implementation of the new GDPR regulation, which sets the framework for client verification and profiling, allows for the creation, development, and implementation of predictive analytics systems on a larger scale.

Currently, less than 3% of voice data is used for the purposes of analysis and creation of consumer models

- According to research conducted by Forty7Ronin (Report: "What You Don't Know Can Hurt You – How to Reap the Benefits of Effective Reporting and Analytics", ©Forty7Ronin Report, December 2017), 53% of contact centre industry leaders think that predictive analytics will be the most influential factor to shape the industry within the next 5 years, even though 40% of all call centre/contact centre institutions still do not own any predictive analytics systems. This shows a significant potential for further development in this area. The basic requirements related to this issue are:

- Assuring the quality of processing the available voice data;
- Proper correlation of available voice data with other consumer information;
- Improving the first call resolution indicator – properly handling customer service during first contact;
- Improving data management and voice channel fraud protection;
- Improving customer experience (CX);
- Improving efficiency by reducing time required for customer service;
- Increasing profits in voice channel sales processes.

High call centre employee turnover is also cited as a very important issue. This results in their low average training and experience level, which causes significant additional expenses related to customer service and employee turnover.

Aside from the well-known automated solutions such as chat bots and virtual assistants, predictive analytics systems are becoming one of the solutions for the aforementioned market challenges. They allow to support telephone agent activities with information sourced from a prediction model as well as the analysis of the ongoing voice call. Another problem, as indicated in the "U.S. Contact Center Decision-Maker's guide" is excessive consumer verification (Report: "US Contact Center Decision-Makers' Guide (2017 – 10th edition)", Contact Babel, 2017). According to the report, in the United States alone, it costs call centres $12.4 billion annually to confirm that a consumer's identity is valid. Predictive voice analytics could help solve this problem by way of identity verification – existing biometric solutions, based on data provided by the predictive system, could decide whether further extensive verification of the consumer's identity is necessary within the scope of the interaction.

In the United States alone, it costs call centres $12.4 billion annually to confirm that a consumer's identity is valid.

Another significant requirement is the creation of a knowledge base regarding calls and conversations. The effective management and use of such knowledge would give customer service agents immediate access to the appropriate information, allowing them to immediately satisfy the demands of the customer. The automated categorization of interactions could be related to the following aspects: reason for contact, mention of competition, behaviour of both sides of call (consumer/agent), use of specific language, keywords, or actions, analysis of emotions and attitude (sentiment analysis) as well as stress and unrest, and any remaining technical information (duration of call, presence of noise, etc.).

The Contact Centre industry covers over 35,000 companies and over 3.2 million jobs. According to a report by ABSL, the total employment level for the first quarter of 2017 amounts to 198 thousand employees in foreign centres, whereas for Polish centres, the total is 46 thousand (ABSL Report: "Business Services Sector in Poland 2017", Association of Business Service Leaders, 2017). In Poland, these centres provide services for 724 institutions. The total number of centres is approximately 1,080, although the number is rising at a rate of approx. 8% per year. There are 47 centres in Poland which each employ over a thousand workers, while the increase of overall employment in this sector is forecast by ABSL to reach 300 thousand workers by the year 2020.

The sector is extremely competitive. Companies providing telephone customer service work at minimum margins, with very strict productivity indicators. Effective agent-consumer voice communication is crucial. A typical, average-sized contact centre, employing a thousand agents, each of them making 40 calls per day, at an average call duration of 3 minutes, would generate 2 thousand hours of recorded calls per day. This constitutes a wealth of information both for call centre operators as well as the clients. Currently, only 1-3% of all calls are monitored by supervisors or analysed by basic automated keyword detection systems.

Voice-driven biometric analytics

Predictive biometrics, particularly when used in business analytics, has only recently become a subject of direct interest of the scientific community. In his work, Fairhurst discusses the systematisation of biometrics as a tool not only for purposes of identification, but also profiling and description (M. Fairhurst, et al. "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data", IET Biometrics, 2017, Vol. 6 Iss. 6, pp. 369-378). It is important to note that biometrics as a technology is not only related to physiological characteristics, but also to behavioural phenomena.

Solutions matching the growing need for the analysis and meaningful use of voice data have been appearing on the market.

Biometric features in prediction systems are any characteristics of a user based on a measurement of their behaviour (behavioural biometrics) or their biological features (physical/physiological biometrics), regardless of whether these features are used as part of security systems or as additional information during the profiling process. They can include the following characteristics of a recorded voice signal: age, gender of voice, height, weight, timbre, intonation (fundamental frequency), prosody, emotion, mood, temper, quality and range of voice (voice spectrum), existence of voice or speech pathology, speed of articulation, rhythm, language, dialect, vocabulary, frequent keywords, and language and articulatory habits. Other information that can be potentially acquired from a recorded signal includes e.g. type of telecommunications channel (e.g. VoIP, GSM, etc.), type and level of ambient noise, type of microphone, acoustic characteristics of device (e.g. smartphone/hands-free set, model of device, etc.). The large amount of available voice data will lead to the development of new methods of the detection and analysis of the aforementioned voice features at an industrial scale, mainly with the use of machine learning and deep neural networks.

From a functional standpoint, the most important opportunities for biometric predictive systems are:

- Use of biometric voice analysis for the creation of prediction models which effectively support business analytics;
- Making use of biometric voice signal analysis (physiological and behavioural) for the purposes of the description and statistical analysis of archival voice data alongside currently used analysis methods (transaction data, analysis of conversation content) and the preparation of useful data on their basis (statistics, reports, statements) for the development of business strategies;
- Making use of prediction models based on biometric voice analysis to monitor a conversation and to adapt to it in real-time, aiming for an optimal scenario of the conversation;
- Making use of prediction models based on biometric voice analysis to detect discrepancies or fraud during a conversation in the active use scenario.

The large amount of available voice data will lead to the development of new methods of the detection and analysis of the aforementioned voice features at an industrial scale, mainly with the use of machine learning and deep neural networks.

The proposed uses of biometrics technologies not only in the scope of feature analysis (better biometrics results, better predictions), but also in the scope of their purpose – biometrics use in anti-fraud prediction, sales and marketing, as well as customer segmentation and trend profiling – are the most important aspects of the current worldwide development efforts.

The rapid development of Artificial Intelligence technologies is a significant factor for this industry, especially in the case of deep neural networks, which are being adapted to new areas of predictive modelling due to the availability of larger amounts of data and computational infrastructures. The technology which is currently researched and planned

to be implemented aims at a uniform deep prediction model (the so-called end-to-end architecture). Its input is to be a raw audio signal sourced from a conversation with a consumer coupled with additional transaction and contextual data, while its real-time output is to consist of actionable information as well as the features and the profile of a consumer, without the need of any further processing of this information in manually defined business analytics processes. Such models are to replace traditional analytics systems in the future, although this can already be observed in the case of social networking platforms (e.g. Facebook, LinkedIn) as well as media platforms (e.g. Spotify, Netflix).

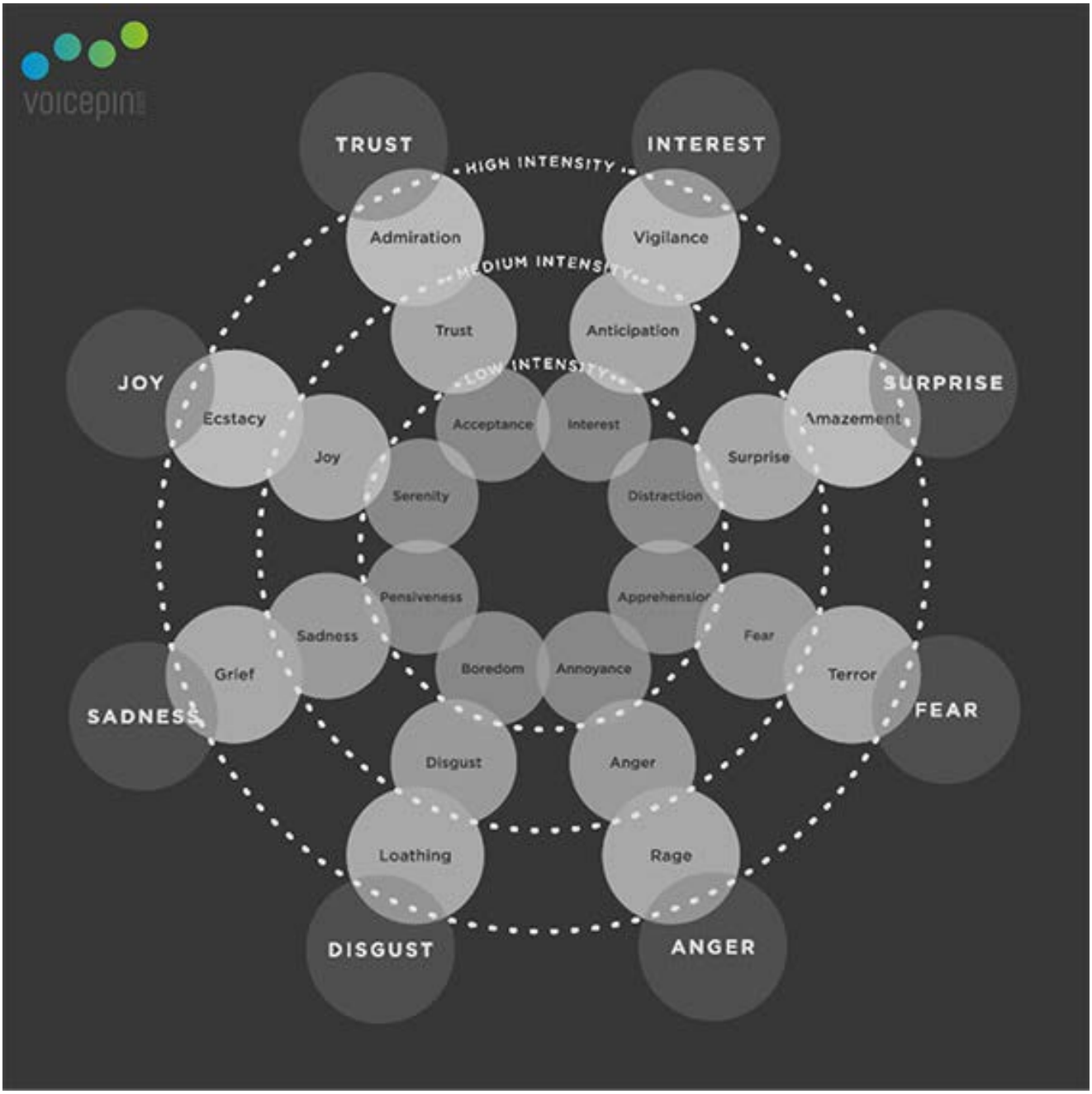


Figure 2. Emotion profiling using behavioral biometric voice analysis

Predictive analytics deployment

Considering the installation and integration of predictive analytics systems, the implementation process will always follow several steps which are common for such solutions. These actions include defining the implementation goal, preparing the prediction models, integrating the system into a business environment, and monitoring the implemented system.

4 – Testing of prediction models.
This is crucial to ensure the system is operating correctly.

5 – Deployment of dedicated system in pilot environment.
This process consists of a practical deployment of the prediction models in the target IT environment.

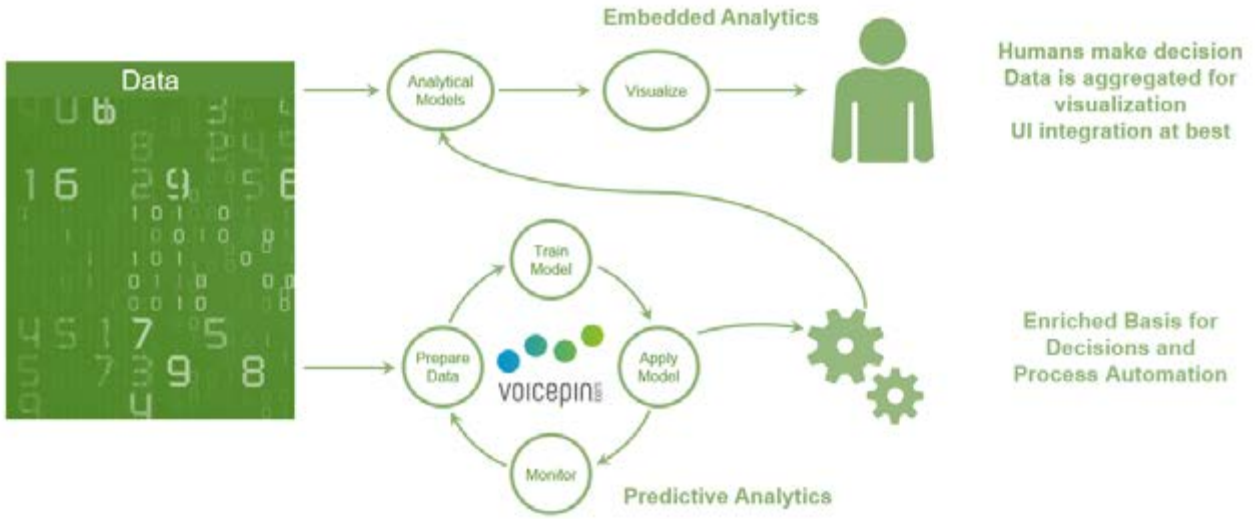


Figure 3. Biometric Predictive Analytics deployment scenario

Box / Frame
Predictive analytics deployment process

1 – Definition of project.
This stage defines the expected results of the implementation project, the scope of its activities, and the business goals, as well as determines the scope of client data available for the creation, development, and testing of particular prediction models.

2 – Data gathering.
This stage consists of the gathering, normalisation (adapting), and initial evaluation of the usefulness (e.g. in terms of quality) of data (particularly voice-related data) to be used for the adaptation of the system's prediction models.

3 – Creation and adaptation of models.
This involves the use of the available data for the creation of dedicated prediction models.

6 – Pilot launch of solution in limited scope.
This allows for testing the system in the target environment as well as its optimisation (e.g. by adjusting particular thresholds or sensitivity levels). It also allows to fix errors and monitor the operation of the system.

7 – Roll-out of system.
This stage involves the deployment of the system in the production environment in its full score (e.g. for all voice interactions, for all processes).

8 – Constant monitoring of operation of system.
This is done with the use of administrative tools and concerns the performance and stability of the system.

9 – Generating reports on effects of prediction.
This includes reports concerning the business indicators of the system's operation. This includes reports concerning the business indicators of the system's operation.

Conclusions

This article has outlined the issues of consumer voice services. It has also described the advantages of the automation of this process as well as the capabilities of biometric predictive systems, particularly in the context of the increase in competition and costs observed in the service sector. The industry is full of unstructured voice data. Being able to understand and use this data is becoming crucial for the optimisation of business processes. Software created on the basis of voice-related technologies allows to make use of the processed and categorised data for the purposes of the creation of profiles and the analysis of the intentions of clients who use voice contact channels. These days, such a functionality may seem like an additional, insignificant change. However, in the near future, the use of machine learning and artificial intelligence will not necessitate making a choice between humans and machines in the case of most companies. Instead, it will constitute an essential symbiotic relationship. ■

ABOUT THE AUTHORS:

Łukasz Dylag – VoicePIN.com[1] CEO, founder. Graduated from AGH University of Science and Technology (Electronics and Telecommunications). He began his career in 2007, being responsible for IVR and Contact Centre implementations in the biggest European companies. Focused on fintech industry trends, multichannel customer experience and security.

Jakub Gałka, PhD – PhD – Architect of the VoicePIN core technology. Scientist, innovator, and speech processing specialist with more than 10 years of experience in speech and data research. He is an R&D Director at VoicePIN and an Assistant Professor at AGH University of Science and Technology. He is a graduate of the Stanford University "Top500 Innovators" programme.

[1] VoicePIN.com Sp. z o. o. is an international market-leading voice biometrics systems producer. VoicePIN offers proven biometric authentication solutions, anti-fraud systems, and big-scale voice-predictive analytics.

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.

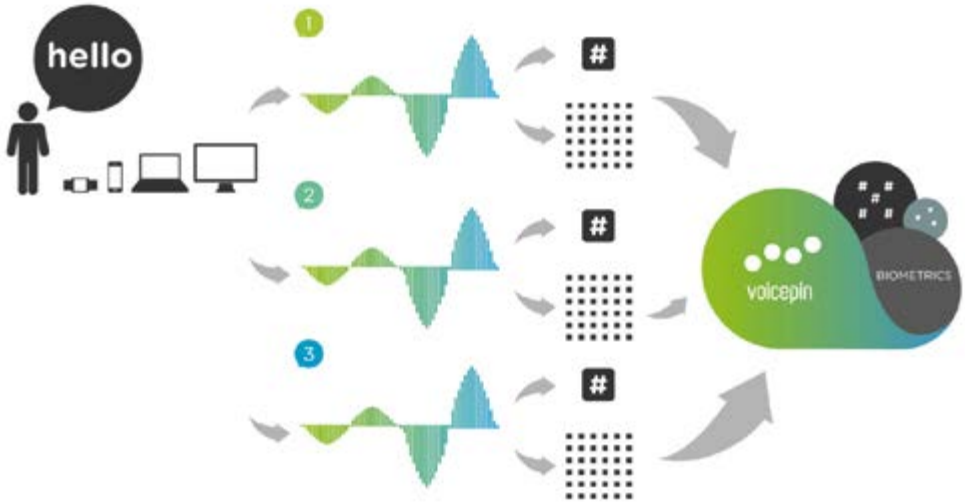
VoicePIN can be used to login, authorize transactions, reset passwords and perform many other security functions.

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

ORGANISATIONAL STRUCTURES OF CYBERCRIME GROUPS: OVERVIEW OF KEY CHARACTERISTICS

BY MATEUSZ MAZELA,
THE KOSCIUSZKO INSTITUTE

Introduction

According to the United Nations, upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organised activity[1]. Media, white papers, cybersecurity reports and other sources constantly provide us with multiple, diverse examples of cybercriminal perpetrators – lone-wolf hackers, cyber mafias and cybercrime companies. However, neither the term 'some form of organised activity' nor the mentioned examples of perpetrators provide us with sufficient knowledge about the cybercriminals' profile or their organisational structures. In fact, a vast majority of sources lack the information which could help us to discover who cybercriminals are and how they operate.

This issue needs to be addressed, as it is necessary to identify cybercriminals' behavioural patterns. In every case of organised criminal conduct, the first step is to understand how the crime is organised: what the members' responsibilities are, what their interdependence is, what the structure of command is, what is their goal, who/what is the preferred victim, etc. Without this information, it is extremely difficult to identify the perpetrators and successfully end the organised crime group's actions. Furthermore, in the case of cybercrime, the lack of information results in difficulties in adjusting cybersecurity strategies to the threat which the company/organisation may face and a failure in properly assessing a cybercriminal group's capabilities.

[1] United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime.* Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

It is estimated that the global cost of cybercrime has exceeded USD 600 billion in 2017. Furthermore, predictions state that a further increase will take place in the following years. These numbers seem to prove that the steps that are being taken to tackle cybercrime are insufficient and ineffective. One of the reasons may be that very little is known about the people who conduct cyberattacks: we know what tools they use, when the attack takes place, and what its purpose is; however, the *modus operandi* stays unrevealed.

It is estimated that the global cost of cybercrime has exceeded USD 600 billion in 2017.

The aim of this article is to present the latest research about the organisation of cybercrime groups and to highlight the need of collecting and sharing more detailed information about cyberattacks between private sector companies and criminal justice agencies. Emphasis should be placed on data that would help to properly assess the level of the threat the cyberattacks may cause and/or to discover the cybercriminals' identities.

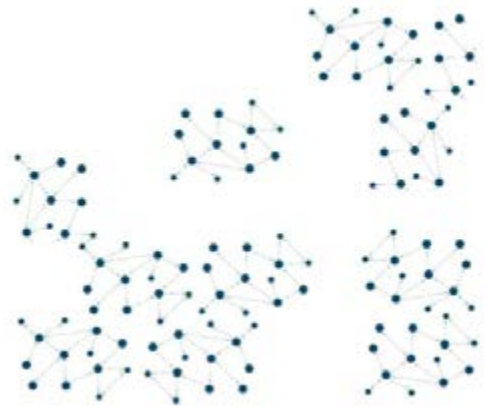
Typology and structures

Currently active cybercriminal groups are characterised by disorganised or distributed models of organisation and have become much more professional and diverse - the cybersecurity threat landscape is stealthier (Rootkits), more automated (Ransomware and Fake AV), much larger (DDOS) and more complex (cloud computing crimes, use of cryptocurrencies, IoT devices and self-deleting communications)[2].

In terms of the organisation, more than a decade ago, Susan Brenner[3] stated that organised cybercrime takes transient, lateral and/or fluid forms. A decade after this statement, McGuire suggested a typology of cybercrime groups, identifying 6 types of structure. It was emphasised, however, that these basic organisational patters often cross-cut in highly fluid and confusing ways and are a best guess, based on the current knowledge about cyber offenders[4]. Furthermore, this typology is likely to change with the constant evolution of digital technology.

Type 1 – operate and communicate predominantly online; reputation-based trust

- Swarms – characterised by many features of a network; described as disorganised entities with a common purpose without leadership. The chain of command is minimal, and they are the most active in ideologically driven activities.



- Hubs – more organised than swarms. Characterised by a clear command structure, which may be hierarchical. They consist of a core team member or members surrounded by peripheral associates . Their activities are driven by profit.

[2] Wall, D. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime*, 2(2), pp. 71-90.

[3] Brenner S. (2002) Organized cybercrime? How cyberspace may affect the structure of criminal relationships. North Carolina Journal of Law & Technology, 4(1): 1–41.

[4] McGuire, M. (2012). Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security

Type 2 – operate both online and offline; described as hybrids

- Clustered hybrids – characterised by crime being committed by a small group of people and focused on specific activities and/or methods. While their structure is similar to hubs, it moves seamlessly between online and offline offences. Their activities are driven by profit.
- Extended hybrids – operate in a similar way to the clustered hybrids, but are more decentralised: their structure consists of many associates and subgroups. The level of coordination is based on the complexity of the operation. Their activities are driven by profit.

Type 3 – operate offline; use cyberspace to facilitate their activities

- Hierarchies – traditional, hierarchical crime groups which use the Internet to support/expand their offline activities. Examples include the expansion of prostitution (pornography, webcams), online gambling, extortion, blackmail, etc.
- Aggregates – loosely organised groups, operating for a short period of time. Technology is used *ad hoc*. An example is the use of Blackberry Messenger (BBM) during the 2011 UK Riots, where the participants organised their operations through the mobile application.

As we can see, the groups differ in the strength of association between members, the environment where they operate and the time frame of the cooperation. In terms of financially driven cybercrimes, the most popular structures are hubs and hybrids. An example of a sophisticated cyber offenders' hub is presented by Chabinsky[5] in Box 1, where the roles of the members are outlined. The question is, is this information still up-to-date, as it has been six years since the report was published?

Box 1

An example of a sophisticated cybercriminal hub/clustered hybrid and its organisation was presented by Chabinsky, a representative of the US Federal Bureau of Investigation's Cyber Division, during his speech:

Coders create malware, exploits, and other tools necessary to commit the crime. Distributors trade/sell stolen data, and vouch for the goods provided by the other specialties. Technicians maintain the criminal infrastructure and supporting technologies. Hackers search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access. Fraud specialists develop and employ social engineering schemes, including phishing, spamming, and domain squatting. Hosts provide "safe" facilities of illicit content servers and sites. Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules." Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location. Tellers assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies. Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds.

[5] Chabinsky, S. (2010). The Cyber Threat: Who's Doing What to Whom?. Federal Bureau of Investigation. Retrieved from https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

In 2015, Wall's[6] summary of the characteristics of cybercriminal groups seems, at least partially, to support Chabinsky's description and McGuire's typology. Wall states that studies conducted in the recent years have highlighted that the members of cybercriminal groups:

- Had specific skill sets and, therefore, different responsibilities within the group;
- Were involved in the work of more than one group at the same time;
- Worked with the same group on a regular basis, but on different occasions;
- Were drawn together by the type of crime, shared interests and/or common goals;
- Were self-contained;
- Were often (but not always) driven by an individual or a very small group;
- Were very reactive in response to circumstances;
- Were bound together by reputational economy.

All of these characteristics fit at least one of the cybercriminal groups' organisational structure; however, hubs seem to have the highest number of similarities.

Another study, conducted by Leukfeldt, Lavorgna and Kleemans[7], analysed the structure of the groups responsible for financial cybercrime only. The results showed that out of a total of 40 groupings, none of them had a strict hierarchical structure *per se*. However, all of them displayed dependency relationships and different functional roles.

In most cases, three different layers could be recognised: core members, enablers and money mules. Core members consisted of a stable group and committed crimes with the same team for a period of time; however, they often simultaneously worked with criminals from other groupings.

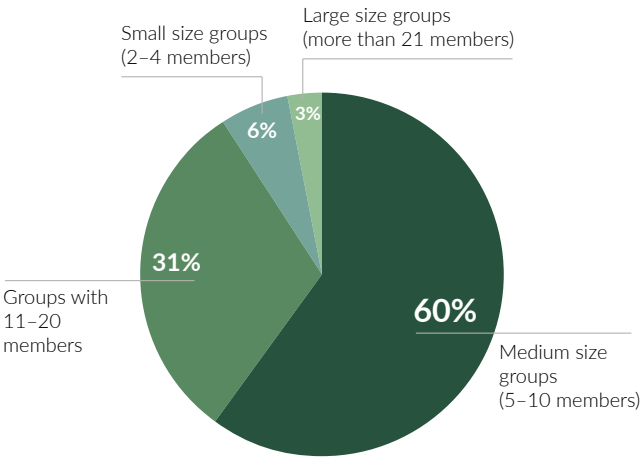
[6] Wall, D. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. The European Review of Organised Crime, 2(2), pp. 71-90.

[7] Leukfeldt, E., Lavorgna, A. and Kleemans, E. (2016). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 23(3), pp.287-300.

In the groups without a stable team of core members, cybercriminals used online forums to find other suitable co-offenders. In these cases, members had their own technical expertise, were active individually on online criminal forums and occasionally worked together.

In terms of the size of the groups, the data gathered during the study led to the conclusion that:

- Medium size groups (5–10 members) were the most popular, accounting for approx. 60%;
- Groups with11–20 members accounted for approx. 31%;
- Small size groups (2–4 members) accounted for approx. 6%;
- Large size groups (more than 21 members) accounted for approx. 3%.



However, the most intriguing finding was related to the role of social relationships. Leukfeldt, Lavorgna and Kleemans presented evidence on the origin and growth of the groups, identifying that, in the vast majority of cases, the groups' structure was based on offline social contacts, and/or offline social contacts were used to create the team of core members, and online forums were used to recruit specialists.

'Offline social ties still play a crucial role in the origin and growth of cybercriminal networks. Core members, enablers, and money mules are recruited using existing social contacts; co-offenders, for example, usually grew up in the same neighbourhood, went to the same church or soccer club, knew each other from the criminal underworld, or met each other in prison,' the authors said.

The picture

The emerging picture of the modern cybercriminal groups' structure is far more than complex. In spite of the fact that, in the case of financially driven crimes, hubs and hybrids seem to be the most popular types of organisation, we have to acknowledge that cyber offenders may be a part of multiple groupings at the same time, and that these groups may use different *modi operandi*. Additionally, as cyber criminals are very reactive in response to circumstances, these groups may stay inactive for a period of time and become active as soon as new opportunities arise.

Furthermore, contrary to the McGuire's typology, type 1 groups do not have to operate and communicate predominantly online, and trust may not be earned through online cooperation only. These elements may be replaced by offline social relationships, which are likely to be present in the organisation of financially driven cybercrime groups. Also, it is important to highlight the fact that this type of groups may not be involved in any types of offline offences.

Finally, the situation becomes even more complicated as a result of the increasing popularity of 'crime as a service' solutions. An example of Carberp – a software tool kit designed to steal from financial institutions, initially developed for private use, accessible only to a small exclusive group of cybercriminals and later available for sale to others – illustrates the way criminal the business model evolves and how the members' roles may be deskilled and/or automated, resulting in their 'distancing' from the crime.

Offline social ties still play a crucial role in the origin and growth of cybercriminal networks. Core members, enablers, and money mules are recruited using existing social contacts; co-offenders, for example, usually grew up in the same neighbourhood, went to the same church or soccer club, knew each other from the criminal underworld, or met each other in prison.

Conclusions

When used to analyse the organisation of cybercrime groups, the reductionism implied by the examples of lone-wolf hackers, cyber mafias and cybercrime companies not only confuses policy makers and private sector cybersecurity companies, but can also misdirect prevention/detention tools and countermeasures. Instead of simplifying the situation, it is necessary to collect data that would help us to unravel the true image of organised cybercrime groups.

As the presented typology is likely to change, it is important to monitor and analyse the situation in order to properly asses the level of cyber threats. The factors on which we should focus on are:

- size of the group;
- strength of association between the members;
- environment where the group operates;
- tools the group uses;
- group's financial resources;
- profile of the victim;
- members' responsibilities;
- hierarchy within the group;
- group's goal;
- using 'crime as a service';
- reactiveness in response to circumstances;
- importance of reputational economy;
- working with multiple groups at the same time;
- time frame of the cooperation;
- social relationships between the members.

This data would help both policy makers and cybersecurity practitioners to assess the capabilities of organised cybercrime groups, leading to the development of more effective cybersecurity strategies. Criminal justice system agencies would also receive tremendous help in identifying and sentencing the offenders. It must be our common goal to gather the information and share it with all relevant stakeholders. Cybercrime is global and knows no borders. Cybercriminals cooperate, constantly develop and export new vulnerabilities. Therefore, successful cybersecurity must be exactly the same. ■

ABOUT THE AUTHOR:

Mateusz Mazela has worked in the Kosciuszko Institute since 2017 as a Partnerships Coordinator. He holds a degree in Criminology (BA Hons) from the Northumbria University. In the field of cybersecurity, he is interested in crime analysis from a psycho-sociological perspective.

CYBER THREAT REPORT CEE 2018

Entrepreneurs, more than any other professional group, should be completely aware that we are entering the era of cyber-dependency, in which the digital frontier will determine our welfare and success. According to several reports, the global cost of cybercrime is expected to exceed 2 trillion dollars by 2019. Bearing in mind that European businesses are strongly affected by this phenomenon, we have conducted a survey among the companies in the region to see how they manage cybersecurity challenges. This report outlines the importance on focusing on ICT security and recommends improving cyber protection for SMEs. It outlines general steps that should be taken, as well as the founding principles of strategies that should be implemented in the realm of cybersecurity investments.

About study

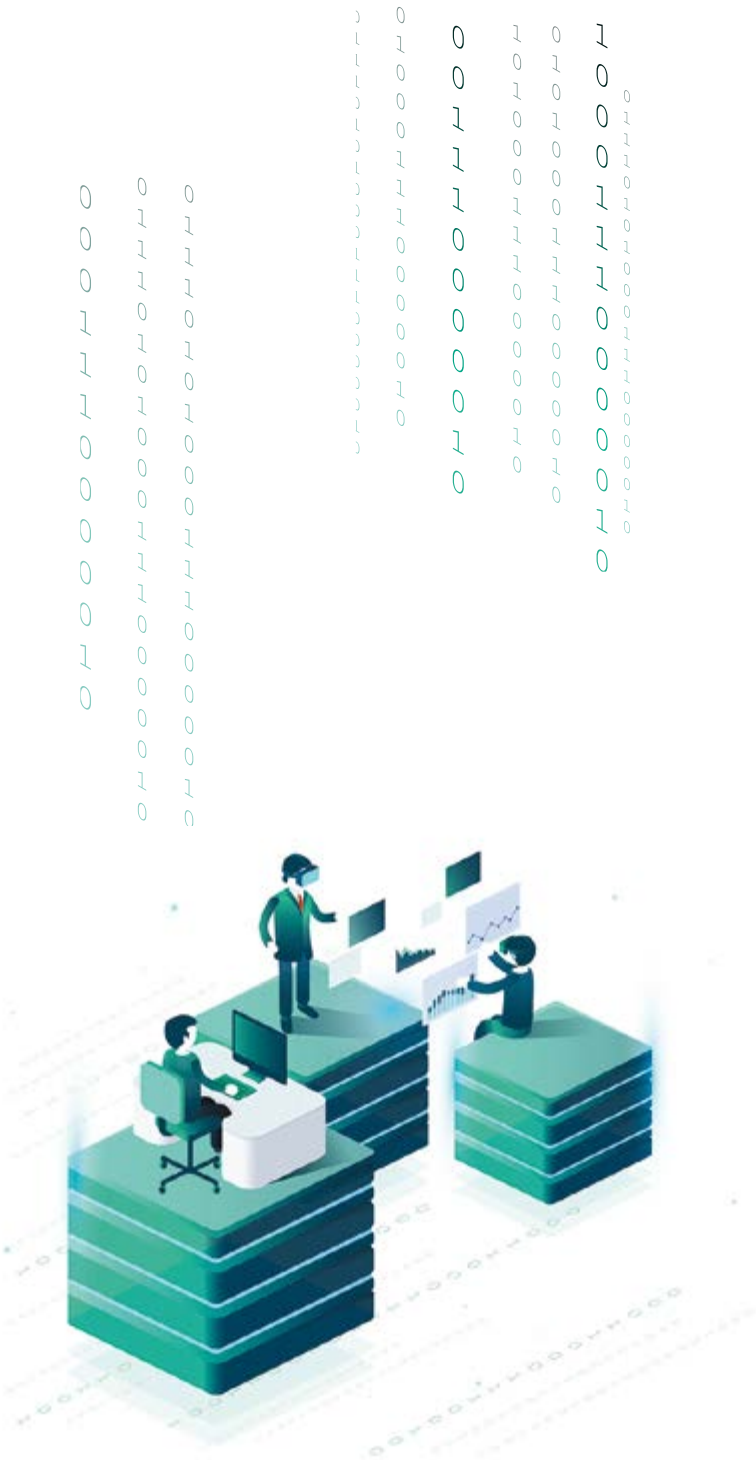
We conducted a survey from March to April 2018 among 500 European companies from the Czech Republic, Poland, Romania, Hungary and Slovakia employing between 1 and 249 people and asked them about cybersecurity-related aspects. We asked senior IT decision-makers several sets of questions revolving around the main topics, such as:

1. What is the total your company currently spends on cybersecurity during a typical year?
2. What is most expensive when it comes to protecting against cyber threats?
3. What types of cyberattacks has your company experienced to date?

The surveyed companies were also asked about the steps they take to protect customer data or whether they have a cybersecurity strategy in place. The results clearly show that most of the companies do not spend large amounts on cybersecurity, which is surprising, especially since we hear more and more about new and sophisticated methods of dangerous attacks and data theft. Another main problem is that a significant portion of cybercrime goes undetected, and criminals are becoming ever more creative in this field.

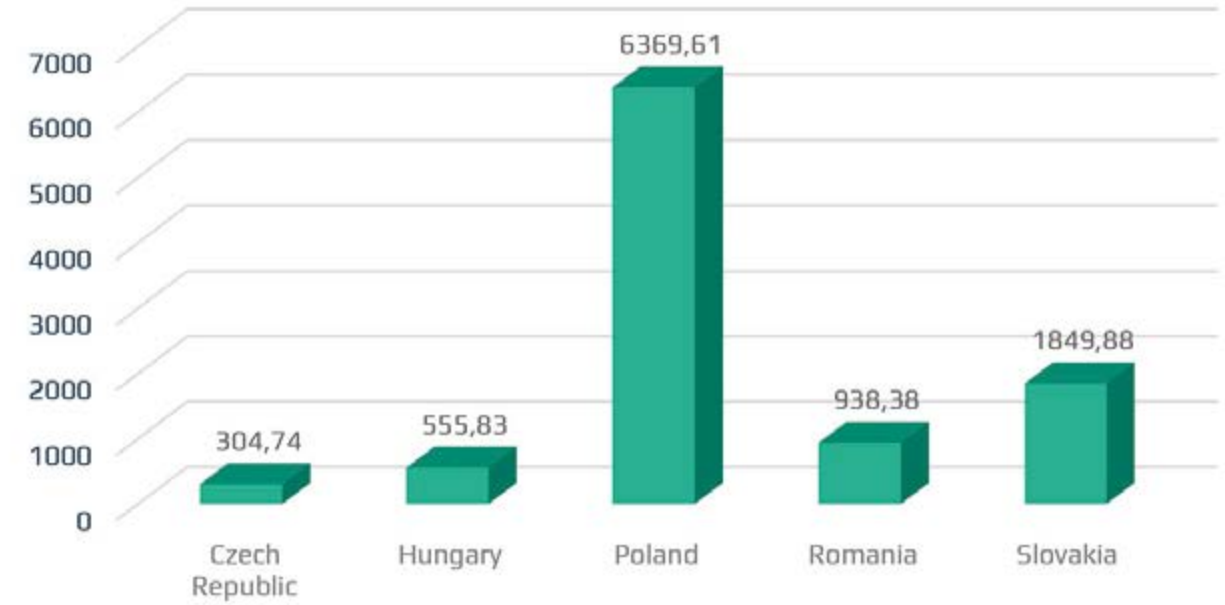
Main observations

In the age of cyberattacks, when there are completely new forms of criminal activities, there is no question that systems need to be designed with security in mind. No matter what industry and what type of data the company works with, they need to take the necessary steps for data security.



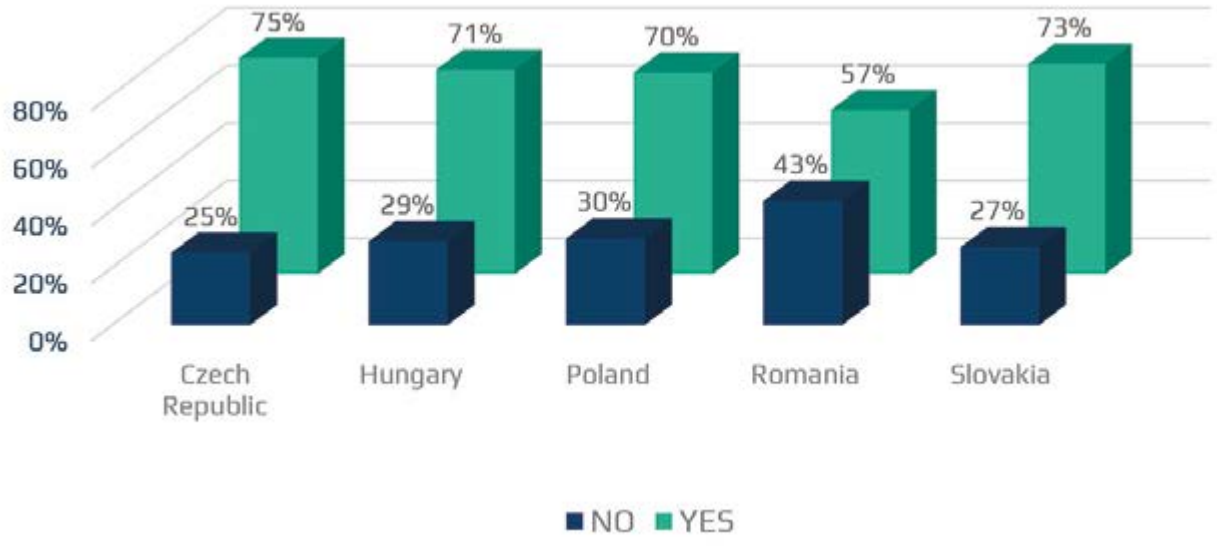
- The average amount spent by companies annually on cybersecurity is EUR 1,966.68, while five years ago, it was approximately EUR 1,908 on average, so little has changed over the years.

HOW MUCH IN TOTAL DOES YOUR COMPANY CURRENTLY SPEND ON CYBERSECURITY DURING A TYPICAL YEAR? (IN EURO)



- In Poland, a high amount of money (EUR 6,369.61 annually) is invested in cybersecurity, but at the same time, Polish companies struggle with heavy losses due to cyberattacks (on average EUR 4,991.72 annually), which affects the average score presented in the study.

DO YOU THINK YOUR COMPANY INVESTS ENOUGH IN PROTECTING ITSELF AGAINST A POSSIBLE CYBERATTACK?

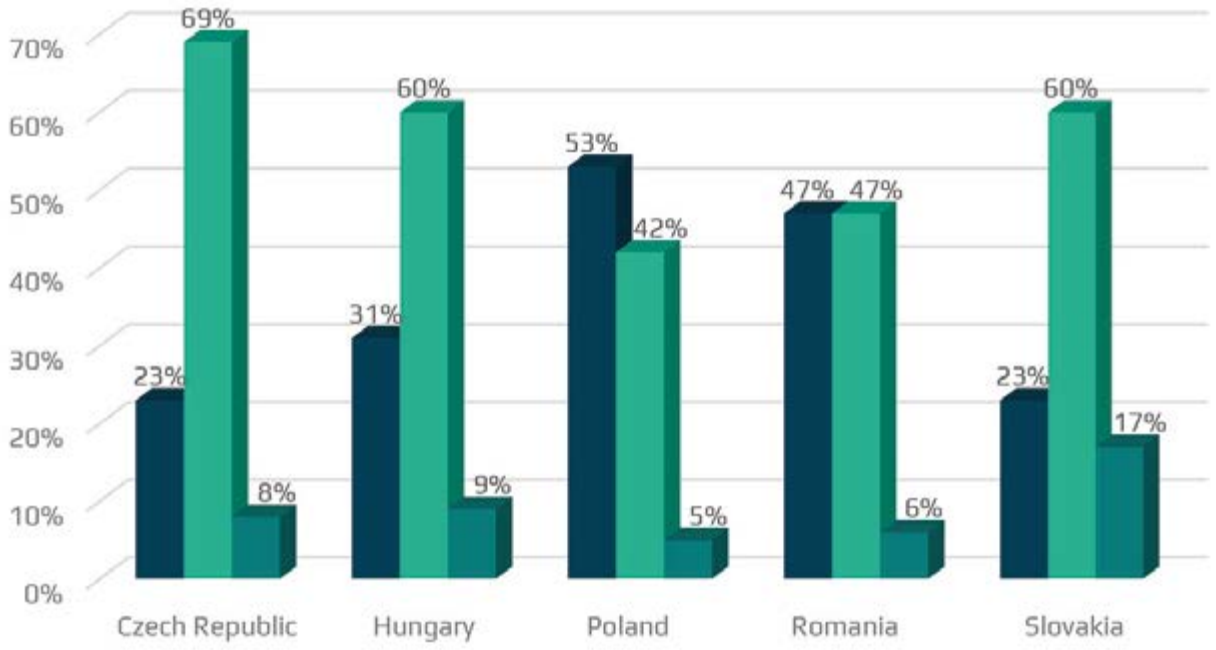


IT security is a headline topic in the media nowadays, so more and more companies are becoming aware of these threats. Not all risks can be mitigated by acquiring sophisticated tools. Especially for application layer attacks, better investments are a proactive approach to security, such as a secure design, security requirements during coding, security testing and – last but not least – building security awareness among developers.

SECURING – WOJCIECH DWORAKOWSKI MANAGING PARTNER

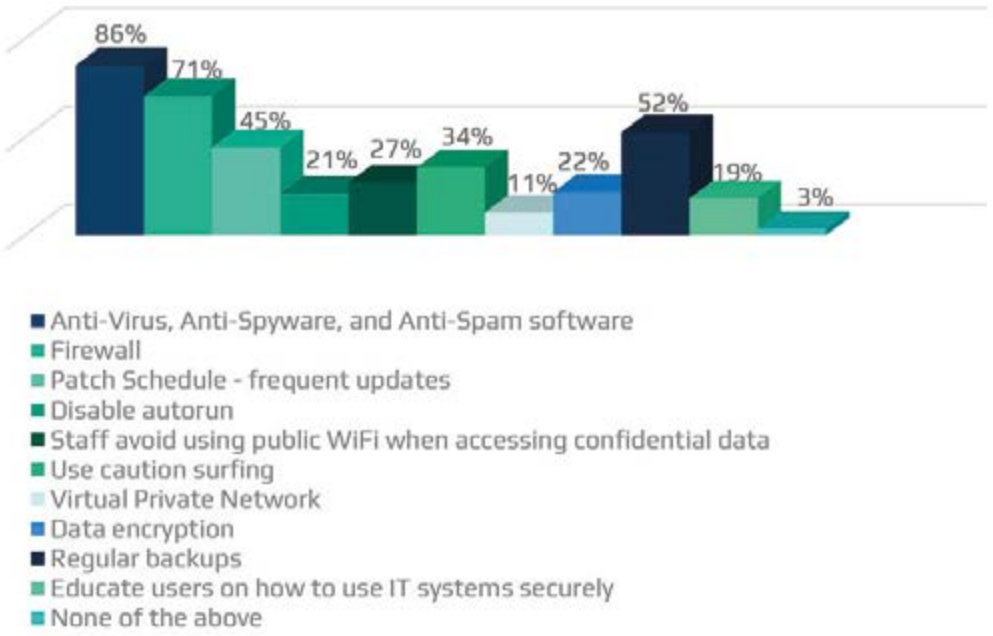
- Most of the surveyed companies spend small amounts on cybersecurity, and only 35% of companies have a cybersecurity strategy for customer data protection in place.

DOES YOUR COMPANY HAVE A 'CYBERSECURITY STRATEGY' IN PLACE FOR PROTECTING CUSTOMER/CLIENT DATA?



- The most popular method among European companies for customer data protection is using Anti-Virus software.

WHICH OF THE FOLLOWING STEPS DOES YOUR COMPANY TAKE TO ENSURE YOUR CUSTOMER DATA IS PROTECTED AGAINST CYBERATTACKS?

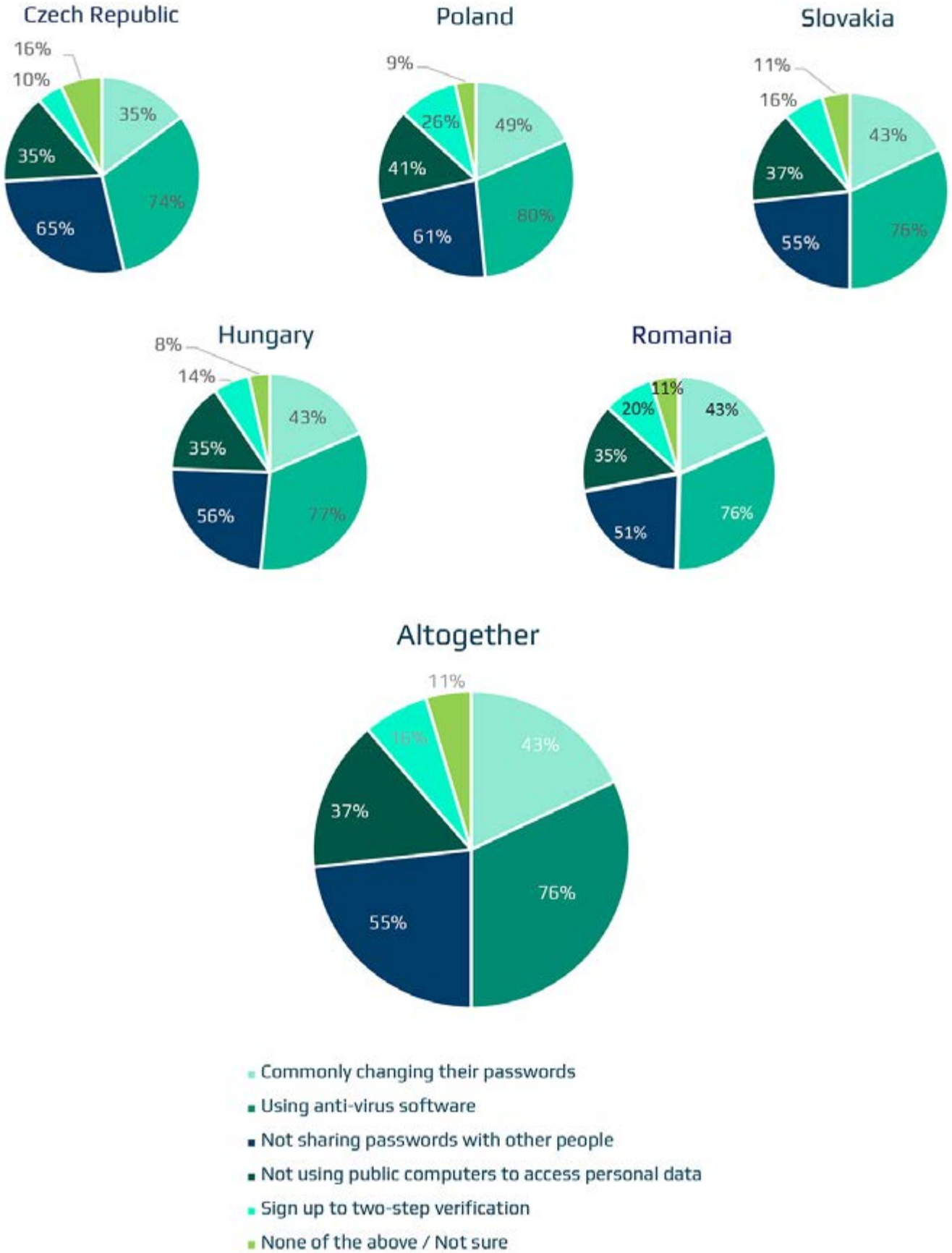


We see that more and more companies and institutions take care of their data using professional backup solutions. At this point, an important issue is not only to make backups, but also to regularly verify the process and procedures, provide restore tests and consider using disaster recovery solutions. The next step for companies is to see and use the value of backup and disaster recovery in their cybersecurity strategy, especially if we think of threats as ransomware.

EWELINA GODŁYN – EXNIT, SALES MANAGER

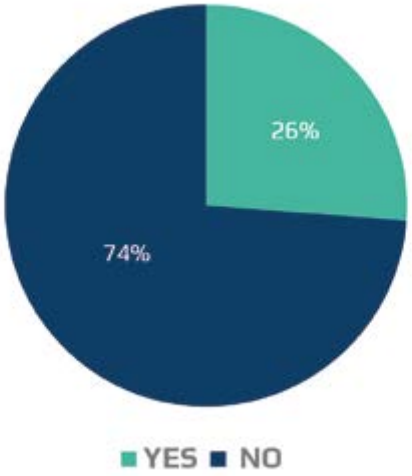
- On average, almost 65% of European consumers still use public computers to access personal data, and the greatest data protection awareness is among the Polish and Slovakian customers.

TO THE BEST OF YOUR KNOWLEDGE, WHICH OF THE FOLLOWING STEPS DO YOUR CUSTOMERS/CLIENTS MOST COMMONLY TAKE TO PROTECT THEIR DATA AGAINST CYBERATTACKS?



- Only 26% of companies feel that they have received enough information and support about the General Data Protection Regulation from the European Union and the vast majority still do not know if they will be ready by May 25, when the regulation comes into force.
  Implementing the GDPR was the most expensive for Polish companies so far (over EUR 6,000.)

TO THE BEST OF YOUR KNOWLEDGE, WHICH OF THE FOLLOWING STEPS DO YOUR CUSTOMERS/CLIENTS MOST COMMONLY TAKE TO PROTECT THEIR DATA AGAINST CYBERATTACKS?



For companies, it is important to gather knowledge, implement relevant solutions and take appropriate steps to fully prepare for potential attacks and to detect them as soon as they are made. Still, most attacks are discovered months after they were conducted and are usually uncovered by external parties.

Companies should include cybersecurity costs into their core business decision making and prepare the strategy wisely, as there is no one-size-fits-all strategy that applies to everyone. Specific business goals should also be the driving force for the ICT security strategy itself, indicating the most important areas of investment. Last but not least, cybersecurity is not only about technology. Education and investments in human capital – employees, clients and business partners – should also be one of the primary parts of building an entrepreneur's attitude towards cybersecurity. ■

FIND THE FULL REPORT AT REPORT.CYBERSECHUB.EU


WHERE CYBER
MEETS SECURITY
CYBERSEC
EXPO 2019
17-18.01.2019
GlobalEXPO Warsaw
CYBERSEC
GET IN TOUCH
Sales Office+ 48 61 847 3755, info@cybersecexpo.eu

CYBERSECURITY MARKET IN THE 3 SEAS REGION

THE DIGITAL 3 SEAS INITIATIVE: A CALL FOR A CYBER UPGRADE OF REGIONAL COOPERATION

THE KOSCIUSZKO INSTITUTE

EXECUTIVE SUMMARY

With the advent of cyberspace, the rules of the game have changed irrevocably. A new arena has emerged where geography no longer restricts individual players. Cyberspace has become another determinant of geostrategic and geoeconomic potential of states.

The authors of the following White Paper call for a range of activities aimed at building digital cooperation in Central and Eastern Europe under the name of the Digital 3 Seas Initiative which would include:

1) **Development of the digital pillar within the Three Seas Initiative should be rapidly enhanced and cybersecurity needs to be included in three pillars: energy, transport, digital.**

2) **Joint cross-border infrastructure projects** (e.g. the 3 Seas Digital Highway) that enable better and more secure data transfer from north to south of the region and bridge the gaps in the communication infrastructure, including fibre optics, 5G technology infrastructure, data islands, complementing energy and transport infrastructures built as part of the Three Seas Initiative projects;

3) Joint initiatives to tackle **integration challenges with new technologies and solutions** that significantly hinder digital transformation of the Three Seas region (e.g. strategic and operational challenges of **cloud computing** integration within the public and the private sector);

4) Development of **common security models and standards for 5G** networks based on the security by design principle;

5) Elaboration on and implementation of the **free flow of non-personal data policy** which underpins innovative and data-driven industry and breakthrough technologies (e.g. Artificial Intelligence, the Internet of Things);

6) **Joint technology initiatives** to strengthen cross-border industrial scientific research and educational cooperation (e.g. autonomous transport, electromobility infrastructure, smart solutions for cities, blockchain) to advance the digital transformation of CEE and the exchange of knowledge;

7) Fostering the **development of Industry 4.0** (e.g. FinTech, cybersecurity, electromobility, HealthTech), which already gives CEE comparative advantage in the global market;

8) Strengthening and securing **e-commerce centres** in locations strategic for the whole region through the construction of smart storage systems and smart customs clearance;

9) Security cooperation on **countering information warfare** based on the common experience and high exposure to hybrid threats within the region;

10) Boosting collaboration, integration and trust among **Digital Innovation Hubs, Competence Centres** and global and regional companies (e.g. developing partnerships and platforms, enhancing the dissemination of digital innovation, promoting matured technologies based on the industry's needs);

11) Boosting the region's involvement in the **development of cybersecurity policies** and strategic concepts at the European level.

Introduction to the concept

Mountains, seas and rivers, which make Europe so enchanting, led to the emergence of an equally diverse political and economic landscape. Geography has always been a decisive factor in determining the economic potential of countries, the location of industrial centres, the shape of alliances, or the delimitation of borders. This is particularly evident in Central and Eastern Europe.

The approach to cyberspace taken by the countries in the region will shape the 21st-century Europe's digital map. Therefore, we can either reproduce the old dividing lines, following geographic boundaries, or build infrastructure that will deepen cooperation. Joint cross-border infrastructural projects, advancements in digital transformation and effective cooperation models within and across countries and sectors will determine the future of Europe. We can draw a digital map that will either consist of modern European states interconnected with digital rivers and the free flow of data, or a collection of alienated states, isolating themselves within their political borders. The success of this process is important not only for the countries of the region, but also for the cohesion of the EU and the transatlantic community.

What is the Digital 3 Seas Initiative?

The Digital 3 Seas is a portfolio of cross-border projects and initiatives that aim to develop digital infrastructure, joint investments and R&D, as well as political and legislative concepts implemented at the EU level. The central idea is the incorporation of the ***security by design*** concept into the digital transition of the public and the private sector. The Digital 3 Seas builds upon transport and energy infrastructure networks that constitute the backbone of the Three Seas Initiative and supplements it with a cyber dimension.

What is the Three Seas Initiative?

The Three Seas (also known as the Three Seas Initiative, 3SI) is a political and economic project inaugurated in 2016 that aims to deepen the integration of the countries of Central and Eastern Europe and strengthen their position in the European Union.

Why does it matter?

The Three Seas comprises 12 EU countries and 114 million of citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion.

The ever-changing global security architecture renders the region increasingly vital for actors as varied as the U.S., Great Britain, China or Russia. Upgrading the Three Seas Initiative by strengthening the digital component, that exists next to transportation and energy components and adding cybersecurity dimension may have geopolitical and geoeconomic consequences far beyond the CEE borders.

The Three Seas is especially important to the U.S. as it will strive to contain the influence of China's Belt and Road Initiative (with the so-called 'Digital Silk Road'). Through the 16+1 format, China seeks to pursue the realisation of the European part of the Belt and Road Initiative and the geographic location of CEE is crucial for building connectivity between Europe and the Far East.

The Digital 3 Seas has great potential to build synergy with such projects as the Digital Single Market, under normative limits and the framework set by the EU.

MAPPING THE DIGITAL 3 SEAS – SECURE DIGITAL INFRASTRUCTURE AND SMART POLICIES

- **The 3 Seas Digital Highway** envisages building a fibre-optic and 5G infrastructure along the already planned transport and energy routes;
- Hubs for services based on **cloud computing** and **data storage** – the so-called **data islands** – could sprout along the **3 Seas Digital Highway**;
- **The free flow of data** would eliminate the necessity to duplicate infrastructure for digital resources storage, thus connecting the **data islands** across the region and enabling the data-driven economy;
- Enhanced secure telecommunications infrastructure together with intelligent storage systems and smart customs clearance could facilitate the creation of **e-commerce centres** near transportation hubs.

IMPLEMENTING THE DIGITAL 3 SEAS INITIATIVE – THE ACTION PLAN FOR 2018:

- **Engaging think tanks and experts** from the region, the U.S. and the United Kingdom;
- Launching the **Digital 3 Seas Business Forum;**
- Crafting a detailed **strategy for implementation** of the digital component into the Three Seas Initiative;
- Promoting the Initiative at **CYBERSEC 2018 in Kraków** (8-9 October 2018);
- Advocating for the digital component to be officially included in the Three Seas Initiative at **The Three Seas Summit in Romania** (Autumn 2018).

THE THREE SEAS INITIATIVE

The Three Seas Initiative (3SI) is a political and economic inter-governmental project aimed at deepening the integration of the countries of Central and Eastern Europe (CEE) and strengthening their position in the European Union (EU). Inaugurated in August 2016 by the President of Poland, Andrzej Duda, and the President of Croatia, Kolinda Grabar-Kitarovic, the initiative is designed to encourage multifaceted collaboration, especially in the area of economics and infrastructure. The Three Seas Initiative comprises 12 EU countries and 22 percent of EU citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion.

Both the Three Seas Initiative and the Bucharest Nine (B9), a cooperation project of the nations on NATO's eastern flank which works on similar principles and have a comparable territorial coverage to the Three Seas Initiative, prove a growing need for establishing a strong regional cooperation framework within the EU.

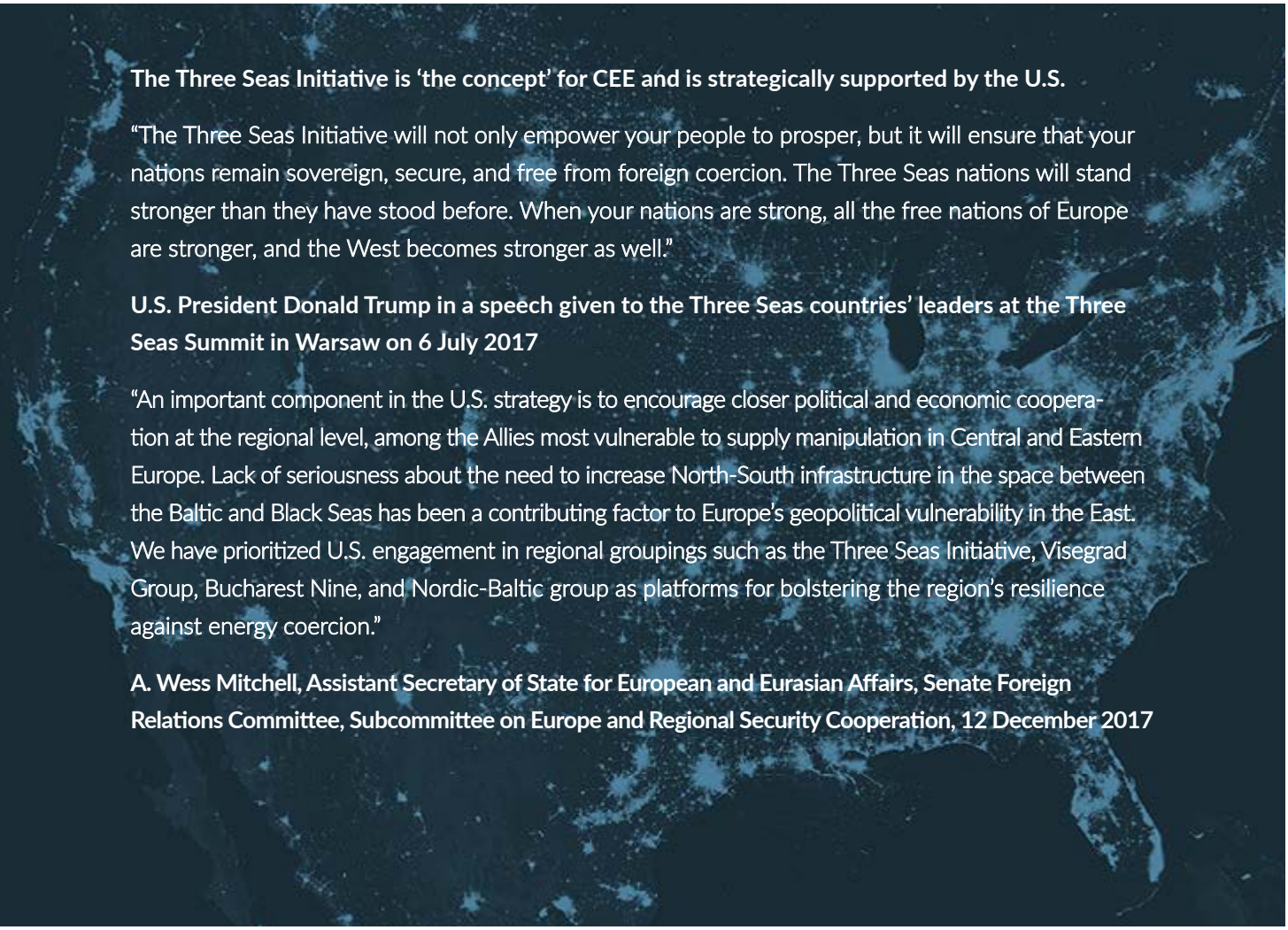
Dynamic digital transformation of CEE economies, an ever-increasing significance of cyberspace in international relations, and new borderless hybrid security threats call for the Three Seas Initiative to be given a strong digital dimension, with a cybersecurity component as its indispensable element.

The threats in the CEE region and the rest of Europe share to some extent a common denominator; however, the CEE region is also a testing ground for some threat campaigns, which can then further resonate geographically. CEE countries, just as any other region in the world, are threatened by various forms of cyberattacks. However, what puts the nations at a particular risk is their greater exposure to conventional conflicts that are increasingly being accompanied by sinister activities in cyberspace, which stems from their location in a geopolitically tense region. The CEE countries that are NATO members strongly advocate for strengthening NATO's presence in the region, seeing it as the guarantor of their safety. A conventional, open military conflict is an unlikely scenario as any decision to launch a large-scale military attack would be extremely risky from the aggressor's point of view.

However, CEE countries are highly exposed to a wide range of cyber operations, not only those that include cyberattacks on information technology (IT) or operational technology (OT) systems, but also those seeking to manipulate people's perception. The reason for that is that CEE countries are involved in strategic, often tense relations with actors who understand and apply cyber operations in a very broad way. History has shown that many cyberattacks, especially those aiming to breach national security, were first carried out in the CEE region (e.g. a large-scale cyberattack on Estonia, disinformation campaigns in Poland, etc.).

The Digital 3 Seas Initiative has potential to foster joint cross-border technological projects, political and legislative concepts at the EU level, as well as scientific and educational cooperation and the development of secure digital infrastructure. Strong regional cooperation is also essential to accelerate the pace and nature of global digital changes. Joining the group of cyber superpowers requires smaller countries to pull resources within a well-structured cooperation framework.

The Digital 3 Seas Initiative should be perceived as such framework and as a complementary project, fitting in with the existing EU schemes, such as the Digital Single Market and the Connecting Europe Facility. The project members should cooperate closely with their partners from the EU and NATO. The Initiative should also be viewed as a unique source of knowledge for Allies because what happens to that region in cyberspace today, is very likely to happen to their homelands tomorrow.



The Three Seas Initiative is 'the concept' for CEE and is strategically supported by the U.S.

"The Three Seas Initiative will not only empower your people to prosper, but it will ensure that your nations remain sovereign, secure, and free from foreign coercion. The Three Seas nations will stand stronger than they have stood before. When your nations are strong, all the free nations of Europe are stronger, and the West becomes stronger as well."

U.S. President Donald Trump in a speech given to the Three Seas countries' leaders at the Three Seas Summit in Warsaw on 6 July 2017

"An important component in the U.S. strategy is to encourage closer political and economic cooperation at the regional level, among the Allies most vulnerable to supply manipulation in Central and Eastern Europe. Lack of seriousness about the need to increase North-South infrastructure in the space between the Baltic and Black Seas has been a contributing factor to Europe's geopolitical vulnerability in the East. We have prioritized U.S. engagement in regional groupings such as the Three Seas Initiative, Visegrad Group, Bucharest Nine, and Nordic-Baltic group as platforms for bolstering the region's resilience against energy coercion."

A. Wess Mitchell, Assistant Secretary of State for European and Eurasian Affairs, Senate Foreign Relations Committee, Subcommittee on Europe and Regional Security Cooperation, 12 December 2017

THE AIM OF THE INITIATIVE:

The Three Seas comprises 12 EU countries and 114 million of citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion. The ever-changing global security architecture renders the region increasingly vital for actors as varied as the U.S., Great Britain, China or Russia. Upgrading the Three Seas Initiative by adding the digital and cybersecurity dimension to already existing ones: transportation and energy, may have geopolitical and geoeconomic consequences far beyond the CEE borders. Development of digital infrastructure in the face of 5G era, joint investments in state-of-the-art technologies such as IoT, blockchain and AI, deepen strategic and tactical cooperation to tackle cyberthreats and disinformation are in the core areas of the Digital 3 Seas Initiative.

PARTNERS OF THE DIGITAL 3 SEAS INITIATIVE:

GLOBSEC is a global think-tank committed to enhancing security, prosperity and sustainability in Europe and throughout the world. Its mission is to influence the future by generating new ideas and solutions for a better and safer world. In an interconnected world, GLOBSEC stimulates public-private dialogue to shape agendas for the future. With global ambitions in mind, and building on its Central European legacy, GLOBSEC seeks to contribute to agendas which are critical for Europe. GLOBSEC acts in the spirit of European values and international cooperation. To this goal contributes the annual GLOBSEC Bratislava Forum, one of the leading conferences on global security in the world.

IRMO

Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

The Institute for Development and International Relations (IRMO) is a public, non-profit, scientific and policy research institute, engaged in the interdisciplinary study of European and international economic, political, cultural relations and communication. Founded in 1963 by the University of Zagreb and the Croatian Chamber of Commerce as the Africa Research Institute, the Institute has changed its name several times, reflecting the changes in scholarly focus. The fundamental mission of the Institute is developing and disseminating theoretical, methodological and technical knowledge and skills required for the scientific and professional interpretation and evaluation of contemporary international relations which affect various human activities and related developmental trends important for the Republic of Croatia. Development tendencies are observed in the local, regional, European and global context. The Institute has 44 employees out of which 16 are tenured academic staff and 7 are doctoral or postdoctoral researchers.

NEW STRATEGY CENTER

New Strategy Center is a Romanian think-tank specialising in foreign, defense, and security policy, a self-financed, non-profit, non-partisan, non-governmental organisation. New Strategy Center operates at three main levels: providing analytical inputs and expert advice to decision makers; holding regular debates, both in-house and public, on subjects of topical interest; expanding external outreach through partnerships with similar institutions and organisations in Europe and the US, joint policy papers and international conferences. The Black Sea and the Balkans space in the vicinity of Romania are priority areas of interest for New Strategy Center in terms of security concerns and emerging opportunities for bilateral and multilateral cooperation. The current activities of New Strategy Center also cover such subjects as domestic developments in Romania as relevant for national security, military modernisation and national defense procurement, energy security and the promises of new technologies, non-conventional and hybrid threats, including cyberspace, and public diplomacy.

SPECIAL REPORT: CYBERSECURITY MARKET IN THE THREE SEAS REGION

The main purpose of the report published by the CYBERSEC HUB platform is to examine the potential of the cybersecurity industry in the EU, with particular emphasis on ten Three Seas countries: Poland, Czech Republic, Slovakia, Hungary, Romania, Bulgaria, Croatia, Lithuania, Latvia and Estonia. The full text of the report is available in polish on the CYBERSEC HUB website.

The report explores in detail the export potential of the analysed market, taking into account such factors as population size, demographic trends, number and turnover of companies, rate of economic growth, labour costs and current level of the region's trade exchange. The report also analyses the ICT industry and the intensity of digital technologies usage by the three main groups of customers of the cybersecurity industry, i.e. individuals, entrepreneurs and the public sector. In the EU, the development of the ICT security market is also shaped by regulatory factors, such as new EU legislation, as well as special market factors related to the wide spread of digital technologies in everyday business and social life; these EU specific factors have are also characterised.

Furthermore, the report attempts to identify the most important trends that will shape the IT security market in the coming years and that may be an opportunity for entrepreneurs. There is no doubt that the industry will develop at a rate well above the average for the entire IT sector. Entrepreneurs operating in the single European market do not have to face many barriers that occur when exporting products or services to customers outside the EU. This does not mean, however, that there are no such problems - they are characterised in the report, as well.

A special chapter of the publication is also devoted to possible forms of support for the export activity of the cybersecurity industry. For example, the problem of the Polish market is not the lack of support instruments for export, but their dispersion within many institutions, which in the case of smaller companies forms a significant impediment. Therefore, the report presents the concept of a nationwide hub of companies from the cyber security industry. One of the key tasks of the hub would be to offer comprehensive services in export for entrepreneurs. The report ends with a discussion of practical issues related to conducting export activities in the single European market through a case study analysis of cybersecurity companies.

Conclusions and recommendations of the publication:

1. The analysis of the ICT sector, including the IT security industry, identified the strengths and weaknesses of markets of Three Seas countries, along with opportunities and threats related to conducting export activities in these countries (SWOT analysis).

2. From the point of view of export possibilities, the strengths of the Three Seas region include:

- Functioning within the framework of the single European market, which automatically eliminates many tariff and non-tariff barriers that occur in trade relations with countries outside the EU;
- Geographic and cultural proximity, which results in, inter alia, intense trade between all EU countries and the region;
- Lower market entry costs compared to Western countries;
- Large fragmentation of the enterprise sector, including ICT, which facilitates the entry of new players onto the market.

3. The weaknesses of Three Seas markets for exporters include:

- A relatively small market, comprising 63 million people, 3.3 million companies and 9 different languages. For comparison, the largest EU market, Germany, has 81 million people speaking one language and 2.4 million enterprises, the revenues of which are about 4 times higher than the revenues of all companies in our part of Europe (excluding Poland). For this reason, entering each of the 10 markets of the Three Seas requires bearing relatively large fixed costs compared to the potential gain;
- Strong local brands in several countries (Czech Republic, Slovakia, Romania and Poland) with high sales potential on the domestic and foreign market;
- Significantly lower profitability compared to Western markets resulting from low margins, which in turn result from similar labour costs in Three Seas countries (in 2018, Poland has the highest minimum wage among the 10 countries in the region).

4. An opportunity for the development of exports on the Three Seas region markets is:

- Significantly higher than the EU average rate of economic development of Three Seas countries in the medium-term perspective, which will increase the purchasing power of companies and individuals;
- Above-average growth rate of the cybersecurity market, resulting, among others, from the growing security threats and new EU regulations; calculated based on data from the European Commission, the import volume of IT security products in 2021 for nine Three Seas countries (excluding Poland) is almost EUR 3.3 billion;
- EU's priority treatment of cyber security issues, which is one of the three pillars of the development of the digital single market;
- Multi-directional development of the IT security industry resulting from multi directional threats, which facilitates finding market niches and specialisations;
- Increasing labour costs in Three Seas countries, which should cause a gradual evolution of the economic model based on low production costs and service provision towards a model based to a much greater extent on ICT, which will have a positive effect on the demand for IT security solutions;
- Catching up in the use of digital technologies by Three Seas countries, especially in the public sector and among enterprises;
- EU funds at the EU (Horizon 2020) and national (structural funds) level to be used by companies from the cyber security industry.

5. The threats related to export to Three Seas markets include:

- Decreasing population: by 2050, the population of 10 Three Seas region countries will decrease by 8 million people;
- Smaller resources from structural funds after 2020 (new EU priorities and UK's exit from the Community).

6. In light of the above SWOT analysis, it seems that Three Seas countries are not treated as a priority direction for the expansion of export among EU cybersecurity companies. Currently, Western markets, due to their size and higher profitability, seem to be a much better market for products and services of the domestic cybersecurity sector. However, taking into account the strengths and opportunities associated with the export potential of Three Seas countries, these markets should be taken seriously by EU companies in the development of export strategies. The low saturation of ICT products and services in these markets, combined with rapidly accelerating digitisation, makes them especially crucial in terms of long term, strategic investments. Vendors who will take active part in the digitisation of the region in the coming years will secure their lasting export presence on those markets.

7. There are four main barriers to the development of exports in the single European market: information (lack of knowledge), market (high competition), finances (lack of funds for starting exports and hedging transactions) and culture (language barrier and unfamiliarity with the realities of doing business in the target country). Various export support instruments are available on the EU markets that address the above problems, including those financed from EU funds.

8. From the point of view of companies in the cybersecurity industry, which are mostly small enterprises, the problem is the lack of human resources (as a derivative of the financial situation) that would be able to comprehensively address the issue of foreign expansion: market research, partner search, gathering information concerning export support instruments, preparation and implementation of expansion strategies, etc.

9. Because it is difficult for individual SME companies to compete on international markets with multinational corporations and local enterprises that have vast marketing budgets (corporations) compared to domestic companies and know the needs and expectations of the clients (local enterprises), the key to the export success of the entire industry is the consolidation of the environment by creating nationwide hubs/clusters/associations of companies dealing with cybersecurity.

10. Today, it is extremely important to build the brand of the entire industry; such actions in the cybersecurity sector have already been taken in France and Germany. One of the tasks of national clusters would also be to create a brand that would support the sale of products and services of each of the companies belonging to a given cluster.

11. It should not be forgotten that innovative products and services provided by enterprises, which, thanks to their quality, innovation and functionality and an appropriate price, meet the requirements of foreign customers, are key for the successfulness of export. Without such products and services, it is difficult to start a discussion about the instruments supporting their sales.

12. Therefore, the issue of designing and implementing pro-export instruments is secondary to the much wider and multithreaded problem of creating a friendly environment for the development of the robust cyber-security sector, which would allow entrepreneurs to take full advantage of their enormous dormant potential. In this regard, the national hubs as spokespersons for the entire business environment would also have a key role to play, stimulating the cooperation of entrepreneurs with the scientific, military or administration sector. Referring to the examples of several countries, it can be said with full conviction that such cooperation is extremely important for the process of mutual learning, creating new products and generating demand for innovative solutions. ■

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION OFFER

Subscribe now and stay up to date with the latest trends, recommendations and regulations in the area of cybersecurity. Unique European perspective, objectivity, real passion and comprehensive overview of the topic – thank to these features the European Cybersecurity Journal will provide you with an outstanding reading experience, from cover to cover.

In order to receive the ECJ, please use the online subscription form at www.cybersecforum.eu/en/subscription

NEW PRICES OF THE ECJ SUBSCRIPTION!

Annual subscription (4 issues) - electronic edition - ~~199 EUR~~ **NEW PRICE 50 €**

Annual subscription (4 issues) - hard copy - ~~199 EUR~~ **NEW PRICE 149 €**

Annual subscription (4 issues) - hard copy & electronic edition - ~~249 EUR~~ **NEW PRICE 199 €**

THE ECJ IS ADRESSED TO:

- CEOs, CIOs, CSOs, CISOs, CTOs, CROs
- IT/Security Vice Presidents, Directors, Managers
- Legal Professionals
- Governance, Audit, Risk, Compliance Managers & Consultants
- Government and Regulatory Affairs Directors & Managers
- National and Local Government Officials
- Law Enforcement & Intelligence Officers
- Millitary & MoD Officials
- International Organisations Representatives

FROM THE FOLLOWING SECTORS:

- ICT
- Power Generation & Distribution
- Transportation
- Critical Infrastructure
- Defence & Security
- Finance & insurance
- Chemical Industries
- Mining & Petroleum
- Public Utilities
- Data Privacy
- Cybersecurity
- Manufacturing & Automotive
- Pharmaceutical

FOLLOW THE NEWS @CYBERSECEU

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