EUROPEAN CYBERSECURITY FORUM

The 2nd Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

26-27 SEPTEMBER 2016 - KRAKÓW, POLAND

CYBERSEC 2016

RECOMMENDATIONS

STATE STREAM

MILITARY STREAM

FUTURE STREAM

BUSINESS STREAM

WWW.CYBERSECFORUM.EU

Ministry
of Foreign Affairs
Republic of Poland

The project is co-sponsored by the NATO's Public Diplomacy Division and the Ministry of Foreign Affairs of the Republic of Poland

Dear All,

The recommendations that you hold in your hands crown the work that was done during the second edition of the European Cybersecurity Forum – CYBERSEC. Thanks to CYBERSEC, Kraków again became the centre for international discussion about security in cyberspace.

During two days of intensive debates, CYBERSEC convened more than 700 people. There were 120 speakers from over 20 countries. Despite different agendas and interests of each group, decision-makers, leaders of opinion, and science and business representatives, have developed practical recommendations that will contribute to reinforcing the quality of multi-stakeholder cooperation and improving overall cybersecurity in Europe. Amongst the leading issues discussed during the event were the implementation of the NIS Directive, the development of a regional system of cybersecurity for CEE countries, cyber defence of NATO member states, fight against terrorism by means of cyber tools, and a growing deficit of cyber specialists.

We truly hope that these recommendations make an inspiring read that will encourage you to become part of the CYBERSEC community and to participate in the upcoming next year's edition, which will take place on 9-10 October 2017.

The Kosciuszko Institute

Methodology

For each thematic Stream – State, Military, Future and Business – there were two Breakout Sessions (BSs) held. Recommendations were drawn up both on the basis of the conclusions formed during each Breakout Session and during four respective discussion panels which enabled speakers to comment on them. The presented material also includes the comments made by the speakers.

Additionally, this year's edition of CYBERSEC featured two special events: a special plenary session held as part of the Future Stream and devoted to investments in the cybersecurity sector as well as a session about combating cybercrime. This document also sums up the key take-away points from the above-mentioned events.
While developing recommendations, the Kosciuszko Institute has made authorial selection of the most significant issues as it was impossible to include all points elaborated on during the discussions. Please note that the recommendations in this publication do not necessarily reflect the views of all CYBERSEC participants.

STATE STREAM

COOPERATION IN THE CEE TOWARDS SUB-REGIONAL CYBERSECURITY: DEVELOPING CONFIDENCE BUILDING MEASURES

Cyber confidence building measures (CBMs) are extremely important tools that contribute to maintaining stability, transparency, and peace in cyberspace. There is a strong need to develop concrete, practical instruments and to operationalize agreed measures. Therefore, the following actions are recommended:

BUILDING ON SUB-REGIONAL FOUNDATIONS

Sub-regional initiatives should play an important role in creating practical instruments and promoting best practices. To enhance overall resilience, they ought to be shared with other sub-regions within the OSCE regional framework. Stable, sub-regional resilience may build confidence both regionally and internationally. The V4 Group has a great potential to become a platform where concrete CBMs are implemented. One proposal is to establish solid mechanisms for critical infrastructure protection and crisis management.

UPGRADING THE TOOLS

The network of policy level contact points among all the OSCE participating states has been established. The next valuable step should be to try out that network by holding joint exercises to find out how the network cooperates and behaves in different situations under different scenarios.

FURTHER INCLUSIVENESS

The efforts to develop cyber CBMs need to adopt a multidimensional and multi-stakeholder approach (with a strong emphasis on industry participation).

ENGAGING DECISION-MAKERS

High level decision-makers are key elements of the cyber CBMs processes and they should be engaged in all crucial aspects of the activities in this field.

STATE STREAM

NIS DIRECTIVE – HOW TO IMPLEMENT THE FIRST EU LEGISLATION ON CYBERSECURITY?

KEY ROLE OF HARMONIZATION

Harmonized standards for the implementation of the NIS Directive should be developed. This process will depend on several factors:

- Effective work of the cooperation group: all Member States should truly get involved and use this platform to develop common standpoints.
- Active involvement of the industry: here the creation of a sectoral information sharing community is recommended.
- An active role of the ENISA: in order to ensure that the ENISA fulfils its role, the agency has to accelerate the revision of its operational model. ENISA must have all resources at hand to effectively tackle this new challenge.

SECURITY MEASURES ADJUSTED TO SECTORS NEEDS

- A sectoral approach should be adopted while implementing cybersecurity measures under the NIS umbrella. Differences and sector-specific characteristics (for example different risks and consequences of incidents) must be taken into account.
- When designing cybersecurity mechanisms, the cross-sector and cross-border dependencies have to be considered.

PUBLIC SECTOR – A REAL PARTER

National authorities in charge of the implementation of the NIS Directive must prove capable of performing the task and being a valuable partner to operators of essential services (OESs) and digital services providers (DSPs). The OESs and DSPs should look beyond cost and view the implementation of the NIS Directive as a beneficial process.

LEARNING FROM EACH OTHER

The Public-Private Partnership on Cybersecurity may be a great forum for Member States, national security agencies and private operators on the demand side to communicate their expectations to the industry about the required needs in order to ensure cybersecurity.

INFORMATION HUB

The establishing of the information hub is recommended. The hub will urge various public entities to step up their information-sharing efforts (for example CSIRTs network, ENISA, CERT EU, and the European Cybercrime Centre hosted by Europol).

CYBERSECURITY IS NOT ONLY ABOUT COST

Regulatory elements must be complemented with a system of incentives.

LIABILITY

A new approach to product liability and telecommunications industry liability should be discussed.

AUTOMATION OF COOPERATION PROCESSES

We have to look for opportunities to further automate cooperation processes in order to enhance response rates and manage risks more effectively.

MILITARY STREAM

NATO CYBER DEFENCE POLICY AFTER THE WARSAW SUMMIT

DECISION IMPLEMENTATION

In order to fulfil the obligations under the NATO Cyber Pledge, it is strongly recommended that:

- Clear goals and the scope of responsibilities are defined at the level of individual Member States and NATO regarding the measurement tools and metrics that will allow them to measure capabilities and assess how their targets are met.
- Investment is made in international capabilities and the upgrade of national defences as well as education, skills, and awareness raising.

COMBATING HYBRID CHALLENGES

While building strong NATO's cybersecurity, hybrid challenges must be taken into account.

- Winning information warfare means recognising the various instruments that has been used to conduct sinister operations in order to prepare an adequate response. It requires strong EU-NATO cooperation and joint effective strategic communication based on true and reliable messages.
- It was proposed that every Member State should have a designated institution that would integrate the efforts to counteract information warfare.
- NATO and its Members should put more emphasis on learning how to react and respond to non-conventional hybrid threats especially at an early stage (Phase Zero) when we do not have a clear view of the situation and when the signs are ambiguous.
- Early warning indicators for hybrid threats should be developed. This effort will require input from different actors equipped with technological, analytical, intelligence, situation awareness knowledge and skills. Building and exercising different scenarios for various situations may be a good practice.

ATTRIBUTION DILEMMA

Attribution dilemma poses a serious problem to international peace. In order to enhance decisions in this area, a few actions need to be taken:

- Further investments in the development of cyber threat intelligence;
- Information sharing (between different actors, including the private sector) that will support technological advancements;
- Further enhancement of intelligence capabilities with a strong emphasis on bringing together civilian and military intelligence agencies;
- Context analysis to determine who is the actual beneficiary of the situation;
- Explore the scope of responsibilities of state actors to provide assistance following the principle of due diligence.

MILITARY STREAM

FIGHTING TERRORISTS WITH TARGETED CYBER TOOLS

BE REALISTIC

It is impractical to assume that we can completely get rid of cyber terrorist threats. That is why a risk based approach is recommended. We need a policy decision preceded by a wide public debate on what the lowest admissible threat threshold is in order to subsequently decide on appropriate surveillance and prevention methods.

ADJUST TOOLS TO THREATS

- Terrorists use the cyber domain for many different purposes; therefore, the tools deployed to stop them must be adjusted to the nature of the threats.
- To fight terrorists spreading their ideology online, we have to not only focus on taking down the content, but mainly work on a counter-narrative.
- The terrorists use online communication channels to plan their operations. In order to effectively monitor these activities and come into possession of crucial information, proactive recruitment of informants must play a key role. We should use traditional intelligence gathering methods and apply them to the cyber world to gather additional information (for example conduct undercover operations in cyberspace). Therefore, the adoption of a cross-domain approach should be endorsed.

THE ROLE OF THE PRIVATE SECTOR

It is up to states to determine what online content can be deemed legal and define what online terrorist content is. Private business is not in a position to make laws. Yet the human rights responsibilities of the private sector must be considered within both national laws (enforced by states) and company policies as direct human rights obligations of private parties, according to the UN Protect-Respect-Remedy Framework ("the Ruggie Principles").

FUTURE

In times to come, the attacks launched by terrorist groups are going to increasingly target integrity of data, not just confidentiality or availability, which means that they will go well beyond website defacements and DDoS attacks and involve acts that are potentially much more problematic and damaging to the infrastructure. It is recommended that critical infrastructure operators are legally obliged to identify and control their critical information assets. They should disseminate best practice and offer tools and frameworks to unmask data manipulation, i.e. means to identify and further control their critical information assets. These "critical assets" are a very limited set of business information (maximum 2% of all information assets). Private companies must identify their critical information assets and processes in order to protect them and ensure they are reliable and trustworthy.

FUTURE STREAM

PREPARING WORKFORCE FOR THE UPCOMING CYBER CHALLENGES

The main recommendations can be presented as a wholly integrated educational value chain. As cyberspace influences all aspects of our life, we should move away from speaking of it in terms of purely IT cybersecurity specialists and start to think about it in the categories of a cyberscience.

Acknowledging cybersecurity as cyberscience is the ultimate goal, but the scheme and approach presented here also apply to the mid stage where cybersecurity is understood in a more conventional way.

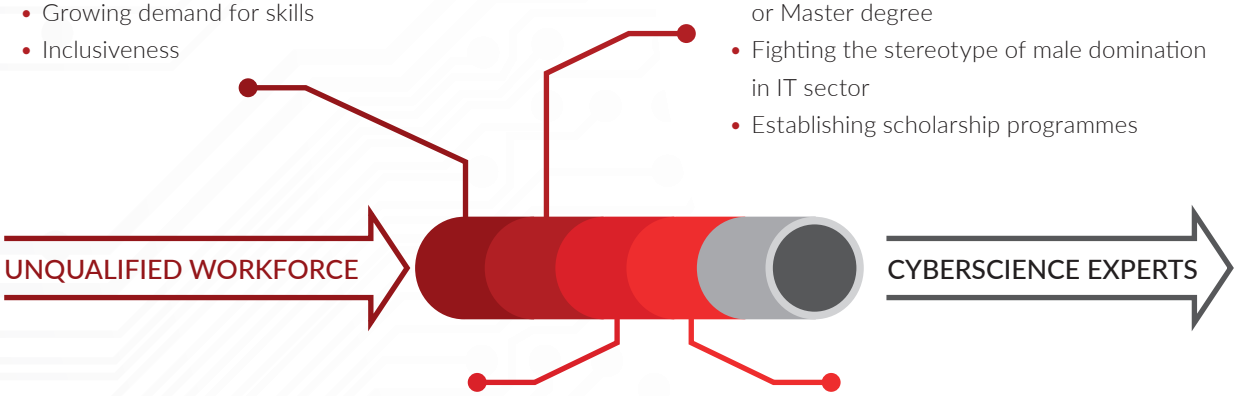
INTEGRATED CYBERSCIENCE EDUCATIONAL VALUE CHAIN

VISIBILITY AND AWARENESS

- Cyberscience visibility as a clear career path
- Real impact on the global economy
- Growing demand for skills
- Inclusiveness

ENGAGING TALENT AT EARLY STAGES

- Capturing and creation of talent
- Encouraging students to take IT as Bachelor or Master degree
- Fighting the stereotype of male domination in IT sector
- Establishing scholarship programmes



DEVELOPING A SET OF INTERDISCIPLINARY SKILLS

- Developing standard skills set for academic Cybersience career
- Certification programmes for Cyberscience specialists
- Promoting interdisciplinary approach to cybersecurity
- Awareness raising and finding one common language
- Establishing Centres for Academic Excellence
- Creating a system of student exchange programs

LEARNING FROM EACH AND PREDICTING FUTURE NEEDS

- Exercising attacks in a controlled ecosystem
- Constant lookout for skills to predict future needs
- Setting-up interdisciplinary teams
- Learning how to respond to cross-border issues
  Establishing scholarship programmes

1st stage of the value chain stimulation is a qualitative change in the **perception of cybersecurity career as an attractive, interesting, and lucrative professional path** that makes a real impact on the security sphere, the global economy, and internal relations alike. It should be promoted as a thrilling adventure and not purely men-oriented and "only-for-geeks" profession.

2nd stage would be the **capturing and creation of talent among different social groups.** It is recommended that talents get hunted and eventually come from a wide variety of backgrounds. This gets us to reach out a very wide scope of people who may not look like promising candidates at first glance.
It is recommended that various scholarships programs attracting young and promising talents are established.

3rd stage involves the professionalization of talents by **developing the "living" set of necessary and interdisciplinary skills** that would not only create high-level professionals, but would also enable them to work together as a team and look at problems from different perspectives (not only IT but also business management, legal, political, etc.). At this stage, different stakeholders should get involved in constant revising and enhancing the curricula for cyber professionals (a strong emphasis must be put on the participation of industry representatives). This will help to always keep up with and understand changing global requirements and needs (market needs but also political, economic, etc.).

In order to catalyse talent development, it is also worth building a favourable scholarly environment, for example by establishing centres for academic excellence that need to meet the national level standards. A valuable element of this initiative at this stage would be a system of international student exchange programs.

4th and last stage, i.e. predicting the future of cybersecurity by learning from each other in real life ecosystems, proves the biggest challenge once we have filled the gap in the supply of highly qualified cybersecurity experts. This is the most sophisticated level in the career development. A great tool to stimulate this process is various exercises with strong interdisciplinary elements. The dynamics of learning from each other not only gives the high-level experts the ability to predict, but it also **keeps a sharp lookout for skills** that are needed to be incorporated into the educational value chain.

The overall challenge that the cybersecurity sector workforce is facing right now is creating a pipeline that would cover all those afore-mentioned processes and scale them up as a standardized process in the global capacity building of professional profiles. Only a complete approach covering all these stages can lead us to success. This complex challenge has to involve all the actors and has to be interconnected with existing initiatives connecting the dots and working together for constant improvement.

FUTURE STREAM

CYBERSECURITY INNOVATIONS – FOSTERING DEVELOPMENT AND COOPERATION

INVESTMENTS

EU level: Financial instruments need customization
Access to the EU funds must be adjusted to the conditions under which innovations arise. Startups are, by definition, founded on the ideas of originality, flexibility and strong work ethos. Creating circumstances that do not suit their nature will kill their potential. Therefore, applying for EU funds where businesses are expected to raise 50% of own capital and cut through all the red tape in order to launch a project that is going to last, for example, 5 years is totally counterproductive. Therefore, it is recommended that financial instruments are better aligned to the needs of small and innovative enterprises.

State level: Public sector as the cyber innovation leverage
Public administration should develop internal knowledge and expertise to be able to appropriately assess investments projects and take risks where necessary. The public sector should develop a VC mindset, namely believe that there are some good ideas worth investing in despite the high risk of failure. The public sector should also provide due diligence to increase trust and further investments in cyber startups. While supporting cybersecurity startups, the public sector should keep in mind that cybersecurity can not only become a source of security, but it can also evolve into as a source of innovation that can drive the innovative economies.

Venture Capital as a central instrument
A favourable climate for VCs ought to be developed at the EU level and at the level of individual Member States alike.

BUILDING NETWORKS

Government should help forge links between academic research and small, thriving companies as showcased by Estonia. Making strong connections with clients is very important and the support of government can facilitate pilot projects and build their initial customer base.

There are different models for establishing much needed cybersecurity clusters and hubs. One of them is a bottom-up approach. Due to its efficiency, it is recommended that this approach is further developed by engaging as many stakeholders as possible.

BREAKING DOWN BARRIERS

There is an acute need to develop dedicated programs that would help startups spread their wings. These newly set-up, fast-growing businesses have ideas and technology skills, but they often lack soft skills that help them reach out to clients and obtain funding. Sometimes the best innovators are not necessarily the best entrepreneurs. Venture capital funds should be encouraged to contribute something more than just money to the companies. Acting as partners, they should help arrange meetings with clients and support risk-taking.

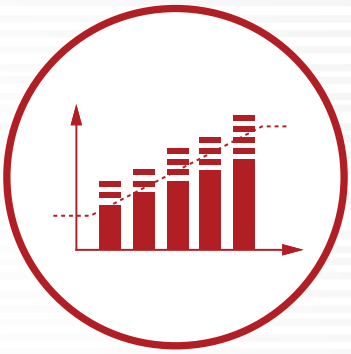
TALENT DEVELOPMENT

The role of academia in cyber is currently largely underestimated and this should change. Institutions of higher education should be recognised as vital talent incubators. A system of scholarships should be created in order to attract the best talents.

INTEGRATED SOLUTIONS

There is a strong trend towards an integrated technology approach in the cybersecurity solutions. This kind of an approach should be strongly encouraged.

BUSINESS STREAM



CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS

IT & ICS INTEGRATION

The perception of security often varies considerably between different groups of specialists within an organisation. Professionals responsible for IT and ICS security tend to take different perspectives to explore the issue. Therefore, mutual understanding and strong cooperation based on regular communication between these two groups must be built. Security and safety perspectives need to be integrated.

TRAINING AND EXERCISES

Joint, routine exercises and training on a micro (companies, operators) and macro level (states) should be organized, with a strong involvement of all the stakeholders (IT, OT specialists within companies, and government, operators, regulators, vendors at a national level).

BESPOKE SOLUTIONS

There is no "one-size-fits-all" solution for ICS cybersecurity. Existing frameworks and best practices may serve as a springboard for developing more mature strategies; however, permanent solutions must be sector specific and based on an effective risk analysis.

SECURITY BY DESIGN

Cybersecurity standards for IoT and ICS should be developed. The principle of security by design is pivotal.

PRIORITATIZATION

While providing cybersecurity, the prioritization of key systems must be ensured.

REGULAR SECURITY ASSESSMENT

Frequent iteration of security assessments is highly recommended. They will help understand better where the deficiencies are in order to take informed decisions about what needs to be done as the next step.

REGULATIONS AND DIALOGUE WITH BUSINESS

All the regulations must be created with a strong participation of business. Only then they may serve as a good starting point to build a mature cybersecurity system within an organisation. In addition to the regulations, business must be strongly self-organised and constantly improve its cybersecurity.

BETTER MONITORING

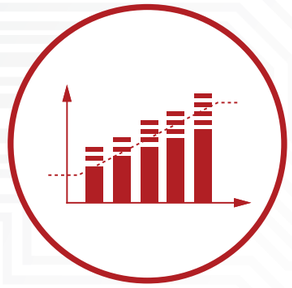
OT networks should be better monitored.

THE ROLE OF INSURANCE COMPANIES

Insurance companies may play an important role in regulating existing ICS cybersecurity practices.

ICS CERTS

National ICS CERTS should be established. They will not only raise awareness and understanding of the threat landscape, but also improve information exchange (anonymous way), and provide necessary expertise.



BUSINESS STREAM

GLOBAL, REGIONAL, AND NATIONAL PUBLIC-PRIVATE COOPERATION – SUCCESS STORIES

QUICK GUIDE TO FORMING PRIVATE-PUBLIC PARTNERSHIPS

JUST START! INITIATE THINGS!

- It is important to start with forming informal partnerships in order to build trust and establish formal partnerships along the way.

SMART DESIGN FROM SCRATCH

- Partnership objectives must be clear and specific.
- Roles and responsibilities of different stakeholders must be clearly defined.
- PPPs should use reliable platforms where stakeholders from the same sector can share and discuss their concerns.
- Recognise that the private sector is the main engine of innovation and involve it in the planning and design of initiatives.

A high level of trust between the public and private entities, which is fundamental to success, translates into a mutual belief in the positive gains for all partners.

OPTIMIZE WORK AND PROCESS

- Recognise that the private sector is the main engine of innovation and involve it in the planning and design of initiatives.
- PPPs must be agile; in order to quickly adapt to changes working groups should be small, their scope of work well-defined and detailed with a clear closed date.
- Follow a bottom-up structural approach for efficient operation that allows for more autonomy at lower levels (local needs and resources).

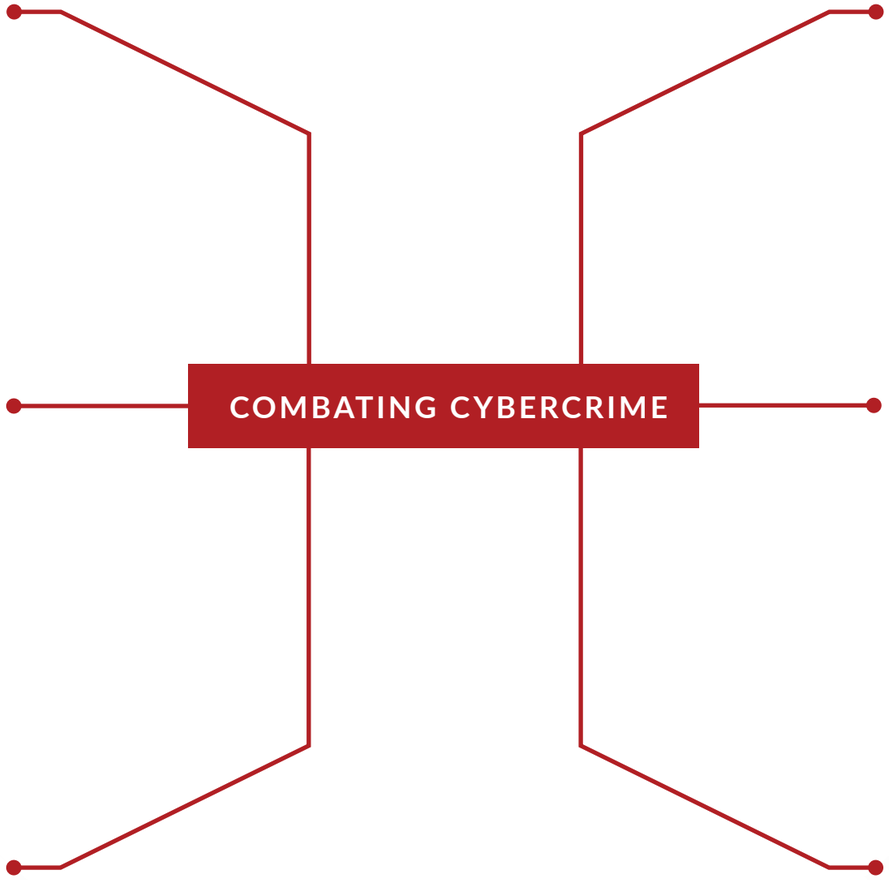
CREATE FAVOURABLE ENVIRONMENT

- Gain political commitment: if politicians understand cyber challenges, they are more likely to push towards decisions supporting PPPs.
- Get influential community involved in the formation of PPPs at all levels of the participating organisations, civil leadership, and the general public.
- Instil “Investment mentality” in PPPs: the private sector must see joint initiatives as a good investment and competitive advantage, not only cost.

While creating regulations, decision-makers must ensure that legislation provides clear baseline guidance. Obligations imposed by legislation should be reinforced with government training programmes and financial incentives.

Decision-makers should consider establishing an EU-level cybersecurity fund. It should be a financial mechanism associated with a research and investment fund.

COMBATING CYBERCRIME
SPECIAL SESSION



Awareness of cyberspace risks must be raised, especially among small and medium-sized enterprises. Although they often fall prey to cyberattacks, they do not invest enough resources in cybersecurity projects.

Harmonisation of the law on cybercrime must be carried out on a global scale. Otherwise we will inevitably have to deal with a growing number of safe havens for cybercriminals, which will significantly hinder effective investigation and prosecution.

It is worth emphasizing that activities undertaken in cyberspace often support traditional crime.

The cooperation between law enforcement agencies and the private sector is still insufficient and must be further deepened. Information sharing culture must be further instilled.

The penalties for cybercrimes should be strict and severe, and cyberoffenders should know they will not escape justice. This is a factor that may hold them back, so legislation and the administration of justice should go in this direction.

Entities should identify their most critical assets and focus on their protection. This is due to the fact that cybercriminals are extremely efficient, which means that we should brace for new types of attacks that will make the protection of all available assets hard to guarantee.

FUTURE STREAM
SPECIAL PLENARY EVENT

INVESTING IN CYBERSECURITY: NECESSITY OR OPPORTUNITY? CAN WE MAKE MONEY BY INVESTING IN CYBER TECHNOLOGIES?

- The public sector plays a crucial role in boosting investments in cybersecurity. On the one hand, the state remains the main investor and capital provider in the cybersecurity domain. On the other hand, with its legislative and executive powers, the state stimulates the development of the cybersecurity ecosystem, as long as it falls into its regulatory-driven investment thesis.
- Money should not be the only value added by the investor in the cybersecurity domain. Equally important, the investor should assist the investee in developing business social networks to help connect with essential stakeholders such as government agencies, academia, and corporate clients.
- Investing in cybersecurity requires specialisation and strong connections with the main public sector stakeholders.
- Different stakeholders of the cybersecurity market should not be antagonised. Investors, be they generalist, specialised, fund-to-fund, or corporate, should be involved in the development of the ecosystem that enables companies to grow.
- European Union's contractual Public-Private Partnership on cybersecurity should not only be seen as a tool to boost investment in cybersecurity and stimulate R&D activity, but also as a chance to define common standards and needs in this field. Even though cybersecurity remains a national competence, there is still room for European cooperation that will contribute to strengthening the cyber resilience system and fostering a competitive and innovative cybersecurity industry as well as the digital single market.
- European cybersecurity innovators need to develop business skills. There are plenty of excellent ideas, creative IT specialists and startups in Europe, but their lack of adequate business skills to attract prospective investors and clients prevents them from reaching their potential.
- The cybersecurity market should not be perceived as a sector purely limited to specific products and services (exclusively cybersecurity solutions). Quite the contrary, the market also encompasses companies that deliver a different kind of value, but with a substantial embedded cybersecurity component (the so-called "security by design"). In fact, one of the requirements of the Fourth Industrial Revolution is that any IT-based solution should include a security component.
- Poland has to find its own niche and build its power and reputation on something that is characteristic and unique to this country only. Therefore, the Polish government must engage in initiatives that promote local solutions and innovations.
- Poland needs to define its competitive differentiation within Europe. The UK has an enormous ecosystem comprising top-tier universities, while in Germany there are multiple cities that are home to companies with established business credibility. Small niche nations such as the Republic of Ireland or Luxembourg offer legislation that provides for the development of privacy protection solutions. Poland has to develop its own competitive advantage within the digital single market.
- Poland should capitalise on its thriving digital entrepreneurship ecosystem as a source of very strong national assets. However, the selection of a cluster within that IT niche that merit further development may be a sensitive matter. Besides cybersecurity, also IoT should be considered as a potential domain to develop national speciality.
- Corporates, large companies and national champions, i.e. state-owned enterprises, should embrace innovative cybersecurity solutions offered by startups. Conversely, startups should provide customer specific solutions and be ready to enter into long-term cooperation with their clients instead of looking for one-off selling opportunities.

CYBERSEC 2016

IN NUMBERS

1 Emerging Public Policy Challenge

2 Days of Thought Provoking Debates

2 Plenary Sessions

2 Special Sessions

4 Thematic Streams

4 Discussion Panels

6 Accompanying Events

8 Breakout Sessions

12 Months of Preparations

16 Hours of Simultaneous Interpretation

20 Hours of Networking Opportunities

20 Countries

35 Interviews for CYBERSEC TV

40 Accredited Journalists

>50 People from the CYBERSEC's Team

>120 Speakers

>400 Articles about CYBERSEC

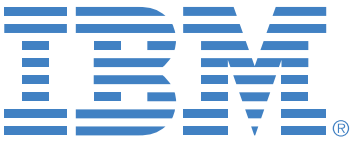
>700 Participants

2800 Photos

79K Twitter Impressions

LEARN MORE ABOUT @CYBERSECEU:

STRATEGIC PARTNERS



MAIN PARTNERS

COMARCH

EXATEL
people behind technology

PGNiG

PKPCARGO

TAURON

THALES

PARTNERS

4ATP GROUP
paloalto networks

25 YEARS GPW
WARSAW STOCK EXCHANGE

arp
Agencja Rozwoju Przemysłu S.A.

CRAY
THE SUPERCOMPUTER COMPANY

ORLEN

PSE

SIEMENS
Ingenuity for life

CYBERSEC STARTUP DAYS PARTNER

CONTENT PARTNERS

SUPPORTING PARTNERS

LOGISTICS PARTNER

HONORARY PATRONS

INSTITUTIONAL PATRONS

MEDIA PATRONS

ORGANISER

PROGRAMME PARTNER

POWERED BY

CO-FINANCED BY

Recommendations were partly funded from PZU preventing fund.

The recommendations are based on the proceedings of CYBERSEC 2016 conference.

We would like to thank all the CYBERSEC 2016 partners as well as Raytheon for supporting the project.

SAVE THE DATE

3rd European Cybersecurity Forum
CYBERSEC 2017

9-10 OCTOBER 2017
KRAKÓW, POLAND

WWW.CYBERSECFORUM.EU @CYBERSECEU /CYBERSECEU