EUROPEAN CYBERSECURITY FORUM

The 1st Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

28-29 SEPTEMBER 2015 - KRAKÓW, POLAND

CYBERSEC 2015

RECOMMENDATIONS

STATE STREAM

MILITARY STREAM

FUTURE STREAM

BUSINESS STREAM

WWW.CYBERSECFORUM.EU

Methodology

The European Cybersecurity Forum – CYBERSEC 2015 consisted of four thematic streams – STATE, MILITARY, BUSINESS and FUTURE. Each stream was divided into two Breakout Sessions dedicated to topics and issues selected during eight webinars featuring panellists that took place prior to the event. The conclusions from Breakout Sessions were presented on thematic panels corresponding to their streams. Beyond that, there was also an additional panel on Combating Cybercrime. The essential thoughts and pieces of information drawn from the panellists' speeches during both Breakout Sessions end each of the thematic panels were a basis for further recommendations.

The Kosciuszko Institute (KI) team, in a co-operation with the session leaders, prepared summaries of each Breakout Session and each thematic panel in a form of draft recommendations. Summary from each session and corresponding panel was sent to its speakers who were asked for comments. Each participant received a document related only to their Breakout Session. Comments were then implemented to the final version of recommendations.

There were two exceptions to this model:
1. Draft recommendations from Breakout Session 1 and 2 in the MILITARY STREAM were combined into one document as the discussion addressed similar issues.
2. Draft recommendations from panel "Combating Cybercrime" have been prepared in co-operation with experts from the Polish Platform for Homeland Security (PPBW). Owing to the fact that it was the special session, additional recommendations have been added by the KI and PPBW experts.

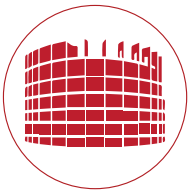
Despite the fact that the Kosciuszko Institute proceeded in the most transparent way and tried to engage all of the speakers, it has to be stated that the recommendations may not reflect the point of view of all of the experts.

Co-financed by

Ministry
of Foreign Affairs
Republic of Poland

The project is co-financed by the Ministry of Foreign Affairs of the Republic of Poland under: „Wsparcie wymiaru samorządowego i obywatelskiego polskiej polityki zagranicznej 2015".

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



STATE STREAM

The creation and implementation of the most important public policies concerned with digitisation and cybersecurity.

#CyberResilience
#DigitalAgenda
#CyberIncidents
#NISDirective
#NIS
#digitisation
#PublicPolicy
#Cooperation
#CybersecStrategy
#CyberSecEU
#TransatlanticCooperation
#CriticalInfrastructure
#CIP
#PublicPrivateCooperation
#CyberSecStandards
#CrisisManagement
#Trust
#InformationExchange
#CyberSecEU
#Interdependencies
#InformationSharing
#EnergySecurity

MILITARY STREAM

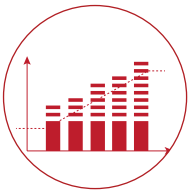
The emerging dimensions for cyber conflicts in Europe - the role of NATO - expanding military cooperation.

#CyberWarfare
#CyberAttack
#CyberArmy
#CyberConflict
#WarsawNATOSummit
#CyberDefense
#NATO
#ConfidenceBuildingMeasures
#CBM
#HybridWar
#InformationWarfare
#CyberPropaganda
#InformationSecurity
#Ukraine
#CyberWeapons
#NATO
#Russia
#CyberCaliphate
#Estonia
#CyberSecEU

FUTURE STREAM

The challenges for the Information and Communications Technology sector and the global information society.

#InternetGovernance
#ICANN
#MultiStakeholder Approach
#InformationSociety
#ITU
#IGF
#InternetCensorship
#WSIS
#FreeOpenInternet
#NetNeutrality
#SmartCities
#IoT
#IoE
#Privacy
#BigData
#DigitalTechnologies
#DigitalMegatrends
#OpenData
#SmarterPlanet
#SmartGrid
#Automation
#CyberSecEU



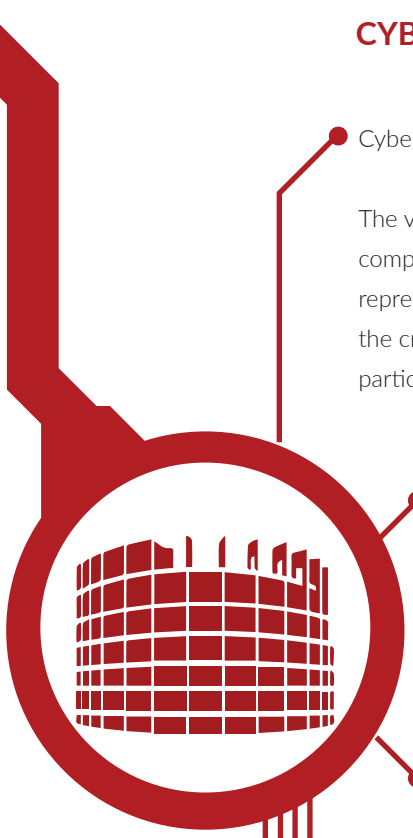
BUSINESS STREAM

Keeping cyberspace safe - the role of the private sector, main challenges, and regulatory framework.

#DGPR
#TransatlanticRelations
#TTIP
#EURegulations
#Trust
#RightToBeForgotten
#Transparency
#FreeTradeAgreement
#IntellectualProperty
#Privacy
#PrivatePublicCooperation
#CyberSecurityStartUp
#R&D
#CloudComputing
#CyberInsurance
#RoleOfBusiness
#CyberResiliance
#CyberInnovation
#CyberLiability

STATE STREAM

CYBERSECURITY CHALLENGES FOR THE MODERN STATE



- Cybersecurity must be seen as a strategic, long term political issue.

  The views on NIS Directive, especially its scope, are divided. Especially the recognition of cloud computing as a critical infrastructure service remains controversial. As a one of the business representatives pointed out – with the growing amount of cloud based services, its inclusion into the critical infrastructure catalogue makes the notion unnecessarily broad. On the contrary, other participant indicated the existence of opposed opinions in regards to this matter[1].

- There is a consensus concerning the need for harmonisation of international approaches. This is seen as the only method that can help to combat transnational cyberthreats. However, strong voices were heard that states are primarily responsible for their own national cyber security. Growing cross-sectoral and cross-border interdependences must be, kept in mind while building national approaches.

- All the initiatives which address cybersecurity should be risked based and oriented towards clearly defined aims. One step that will help achieving this goal is to understand and specify the threats.

- More funding needs to be allocated on cybersecurity. One proposition is to apply a rule known from the area of conventional security (chosen percentage of GDP spend on security – in this case cybersecurity). This approach can be considered both at national and international (NATO, EU) levels.

- The pull of cybersecurity workface must be increased. State should stimulate this process.

- Users must understand the cyberrisks and they must use the ICT products and services with greater awareness. In order to achieve this aim education is needed. It is recommended that every Minister responsible for education make sure that cybersecurity is integrated with the whole educational cycle.

- Security language should be translated into business language – a management board must not only understand the importance of cybersecurity but also see it not only as unnecessary burden, but also as a profitable investment.

1. For example this document was pointed out: https://www.enisa.europa.eu/media/press-releases/new-enisa-report--the-double-edged-sword-of-cloud-computing-in-critical-information-infrastructure-protection

INFORMATION SHARING

- There is a clear and broad consensus among business, state and civil society on the need to share information. Information sharing should be at the center of the new, more proactive security model.

- At the same time the views on mandatory vs. voluntary reporting are divided. Business tends towards the voluntary model, finding the mandatory one too quantitative, and therefore missing the actual core of the problem. In the mandatory model, business might tend to provide only the numbers of incidents, as required by law, rather than offer practical insights into solutions to current problems. Cyberspace can be seen as too dynamic for regulations. Governments argue that the voluntary model fails due to lack of business engagement (low participation) and would rather obtain a clear set of information from all critical services operators on mandatory bases. There is a need for further dialogue on the appropriate model of reporting cyberthreats.

- Keeping in mind these differences, some recommendations on effective information sharing can be presented.Especially the following elements are crucial:
  - Shared information must in a real way contribute to the solving pre-defined problems. Stakeholders must know what kind of information is needed and why (what kind of problem will be solved).
  - Cooperation and information sharing must work as a win-win model. Information from the public sector should be shared on equal basis with those from the private one. The current regulation excluding public information from dissemination is perceived as unfair.
  - Governments should provide a clear plan for processing the security data obtained from private sector and based on this data, they should provide effective input into the cybersecurity dialogue. All the parties involved must see clear results of the cooperation.
  - States should play an important role in sharing information during a crisis situation.

- There is a need for enhanced debate on the necessary limits of trade/business secrets vs. cybersecurity reporting. There is a need to enhance awareness of the fact that sharing information on cyberincidents rather than hiding away the damage caused by cyberthreats serves the benefit of all parties involved, including the victims. For now there is a tendency to hide the effects of cyberattacks rather than share information on the details of the attacks – companies and public bodies alike are reluctant to show their weaknesses in the field of cybersecurity. Yet, only through information sharing, current threats can be addressed to the benefit of all. Therefore this current tendency should be addressed and reversed.

- The question of funding additional cybersecurity efforts, required from the private sector, remains open. Business argues that if a state introduces additional security measures it should also provide the means to have them operable.

- Private – public cooperation and discussion must include legislative decision-makers as well as academia.

INTERNATIONAL COOPERATION AND THE NEED FOR CYBER-DIPLOMACY

- In order to effectively conduct international cyberprocesses, states and the EU should develop their own cyberdiplomacy.
- Cyberdiplomacy must be open to different stakeholders.
- The crucial element of the international cooperation is capacity building. Development policies must be integrated with security policies in order to increase overall level of cybersecurity. Funds for development must be spend also on cybersecurity.
- There is a noticeable lack of exchange of information on sources of online threats, including their geographical origins. Therefore there is a growing need for enhanced diplomatic efforts in this area.
- We need to develop regional and global mechanisms of cooperation and work on common behavioral norms. CBMs are god example of this kind of cooperation.
- Cyberexercises must be further developed. In order to stand against hybrid warfare, it is recommended to discuss the possibility of joint exercises between NATO and the EU.

STATE STREAM

CRITICAL INFRASTRUCTURE CYBERSECURITY PROTECTION

GENERAL APPROACH

- It is states' responsibility to identify and designate critical infrastructure. International organisations like the EU should rather aim at harmonization of definitions and some general approaches.
- It must be noticed that not all critical infrastructures are equally critical. States should identify these, which are absolutely important for the economy, citizens and state functioning. Protection of these elements should be prioritized.

- Information sharing (widely understood) is identified as a fundament of success in context of critical infrastructure protection.
- As a one of the participants pointed out, the role of the state is to create legal environment enabling efficient and transparent information sharing between different stakeholders.
- In order to design and implement well working information exchange, states must precisely define what they want to achieve, what kind of problem they want to solve, and what kind of information they expect to receive, in order to meet the goal. Expected results must be clearly outlined – so called targeted information sharing approach is strongly recommended.
- Success of information sharing depends on quality of information that will be exchanged. Information must be relevant and timely.
- The most important element of domestic and international cooperation is to build trust among different stakeholders. It is valuable to meet personally and get to know the counterpart. The EU may be facilitator but solving the problems especially via bilateral contacts are the most effective.
- The absolute precondition of successful information sharing is protection of privacy and sensitiveness of information. Involved actors must be convinced that exchanging information will not do the harm to their business and their clients.
- Traditional way of the governments' acting must be changed. Exchange of information must take place in two directions – private sector must not only deliver data but also receive relevant and reliable information. Private sector must be an equal part of the system.
- It is important to establish different levels of information sharing. One proposition is to have regional, sectoral and national/strategic platforms.
- National and international cyberexercises play important role in the process of establishing and testing information sharing. It is recommended to involve in the exercises all crucial stakeholders (including political decision-makers).
- Critical infrastructure operators should start to seek platforms to exchange information and develop sector specific standards. Both tasks should be align and, in the future, achieved through Network and Information Security (NIS) Directive guidelines.

- There is no consensus in terms of the need of regulations in the area of cybersecurity. Both approaches – voluntary and mandatory have pros and cons. Also different countries have its own specific characteristic, maturity and circumstances. It is recommended that each country should decide which way they want to choose. One of the participants claimed that state have to clearly define minimal standards for the protection of critical infrastructure and must have means to control and measure the compliance of the operators with these standards. Not everyone supported this position.

- While developing standards for cybersecurity, the role of private sector is crucial. Business must be involved in the process and this process must be built on a dialog. States must point out what to do, not how to do it. When the state says how to do it, the state bears the cost.

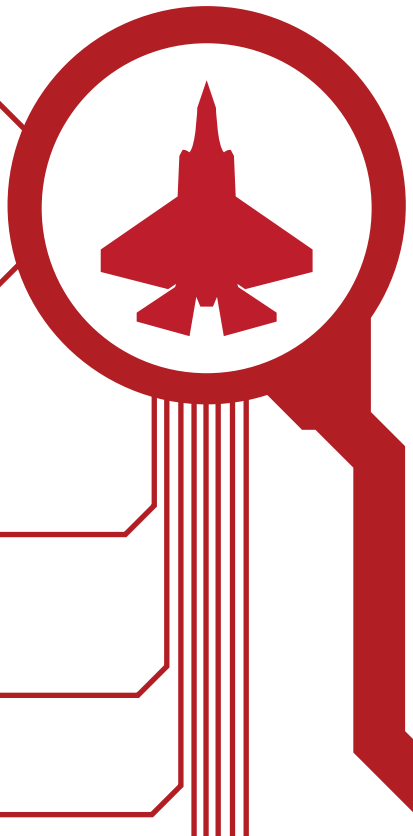
- Because all environments are different we should focus on a sector specific standards. Preparing recommendations is especially important for small and medium companies which often can not afford to prepare own tools.

- Most of the participants stated that additional funding of the CIP from the states' budget is not necessary. What is more important is to create system of incentives that will encourage business to engage even stronger in CIP.

- The panelists agreed that an area which is becoming more and more important and crucial in regard to cybersecurity is the protection of SCADA systems, which are a driving force behind the majority of critical infrastructures.

MILITARY STREAM

CYBERWARFARE – FIFTH DIMENSION OF ARMED CONFLICT AND CYBERTHREATS IN EUROPE



- There are at least a few roles of military in state cyber activities:
  - Own military assets protection
  - National defence
  - Under state of emergency procedures/legislation, support in major crisis management
- There are at least 4 perspectives on cyberarmy activities:
  - Situational awareness
  - Defence and protection of military information resources
  - Conducting cyberwarfare
  - Cyber actions must be integrated and support all the other military operations
- Cyber strategies must serve as a basis for decisive and solid executive actions. Strategies alone are not sufficient. They should be regarded only as the first step to provide cybersecurity, foundations for efficient cyber defence measures, institutions, forces.
- Governments should establish principles and processes for cyber operations, both military (cyberwarfare) and crisis response (defence against cyberattacks not amounting to armed attacks).
- Transparent cybersecurity strategies enhance the stability of global cooperation and understanding.
- There is a need for harmonising NATO Member States' national strategies and doctrines.
- There is a need for establishing political cybercrisis management framework to ensure that the response to such cybercrisis remains proportionate to the threat.
- There is an increasing trend in investing in and development of national cyber capabilities - relying on national security products and capabilities rather than imported ones might increase the level of security.
- As history showed especially on the example of conflicts in Ukraine and Georgia – cyberspace can be utilised in many different manners e.g. for espionage purposes as a tool for information warfare (propaganda, disinformation etc.), and probably as a destructive force. It is also clear that there are various objects of cyberattacks.
- Terrorist groups use Internet to perform their activities more and more often. So called Islamic State massively uses Internet for ideological purposes, data mining, recruiting and other activities, including psychological warfare. States must find the way to respond to these threats. It has been proven that old-fashioned mechanisms like censorship does not work.

NATO AND STATES CAPABILITIES

- In order to build effective NATO capabilities, nation states must firstly enhance their own capabilities within both defence and offensive actions. By Article 3 of Washington Treaty, member countries are obliged to build their own cyber capabilities, as reiterated in the Wales Summit Declaration. Strong nations constitute strong NATO.
- It must be underlined that offensive actions can serve for both defensive and deterrence purposes. Currently, in accordance with Enhanced Cyber Defence Policy, NATO does not allow to take offensive cyber actions and develop offensive cyber capabilities. Therefore, the decision of possible development of offensive cyber capabilities has to be discussed and made on the national level.
- The development of offensive cyber capabilities expands the arsenal of possible responses towards possible aggression.
- Discussion on invoking Article 5 of the Washington Treaty should take under consideration that cyberattack, because of its specific character, cannot be equated with the conventional attack and must not always be understood as a call to collective defence. The reaction always requires wide debates and consideration of various scenarios.
- Nations must develop their own centres of competences, in particular, in areas of cybersecurity, as stated in the Wales Summit Declaration "[...] responsibility of Allies to develop the relevant capabilities for the protection of national networks.". This contribution of national capabilities would help to build overall NATO potential. It is recommended that all member states sign second generation of Memoranda of Understanding (MOUs) addressing this issue.
- NATO Specialised Cyber Defence Force should be built and trained, in a manner similar to NATO Response Force.
- NATO should consider creating Cyber Component Command aside from the existing Land, Air, Maritime and Special Operations Component Commands.
- NATO and nation states must make it more costly for perpetrators to conduct cyberattacks.

COOPERATION

- Nationwide cyber exercises engaging private sector are needed.
- Framework for the protection of critical infrastructure must be established. Crucial element is to define roles and responsibilities of military entities, civil entities and private sector.
- Clear and actionable programme of information sharing must be in place.
- Incentives for more effective information sharing (also with the private sector) must be established and based on the fair trade rules.
- In terms of information sharing – common case study databases can be created, similar to NATO's Cyber Information and Incident Coordination System (CIIS). Stakeholders should be encouraged to share not only the success stories but also the best practices resulting from failures. Access to data should be proportional to the readiness of sharing.
- Voluntary civic defence leagues as a great form of civil – military cooperation should be established, paying due attention to the provisions of International Humanitarian Law (Law of Armed Conflict) regarding taking direct part in hostilities.
- Private – public cooperation must take into account one element – combatant immunity. There must be a clear cut between cyberdefensive activities of the civil sector and cyber warfare.
- State level cooperation should be developed with respect to the existing competence capabilities of the cooperating parties.
- As cyber operations are often a part of broader geopolitical conflicts – therefore by analysing international situations we need to take into account possible cyberimplications.
- In this terms cyberdiplomacy must be build. In order to establish its priorities framework established at the EU level may be taken into account.
- Initiatives similar to NATO Industry Cyber Partnership (NICP) should be widely promoted with the aim to decrease the time required for Nations to develop their cyber response capabilities, based upon the results of research and development programmes already run by industry and academia.
- "The legal framework governing the conduct of hostilities in cyberspace is sufficient (in terms of international law, including treaties, customary international law, states' practice and jurisprudence of international tribunals) and the tendency to over-regulate should be avoided. Nevertheless, peaceful use of cyberspace and in particular enforcement of criminal law in cyberspace might require more detailed framework to get closer to a zero-tolerance on illegal activity. The US-China bilateral agreement might serve as an example of how to regulate without restricting the freedoms offered by access to the World-Wide Web. The most grave cybercrimes could be considered as a falling under universal jurisdiction, similar to piracy or human trafficking".

- There is a need for smart R&D in the area of cybersecurity, in close cooperation between state agencies and industry and academia. Priorities and goals must be set up and the proper funds must be assured and it should be based on the existing cyberdefence capabilities of cooperating parties.
- Priorities of investment in increasing cybersecurity capabilities should be cyber resilience, flexible network architecture and equalising potential.
- Analysis of typical phases of APT (Advanced Persistent Threat) attack may help to increase the level of cybersecurity. Different actions must be taken in the different phases of the attack.
- Cyber intelligence capabilities as well as situational awareness should be developed. This will help to resolve the attribution problem and it will shift reactive defence towards more proactive approach. As the private sector is very well developed in this area, the PPP approach should be used for this.
- Cybersecurity is all about talents – system of higher education must be adjusted to this need.

FUTURE STREAM

INTERNET GOVERNANCE - CYBERSECURITY ISSUES

- There was a rather broad consensus that the definition of Internet Governance introduced by WSIS (see below) is correct and there is no need to provide significant modifications in this respect.
- "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".
- Some participants thought that identification and clarification of roles and responsibilities of different actors in the area of Internet Governance also seen from the cybersecurity perspective would bring added value to the debate. Especially taking under consideration the fact that this environment is very complex and consisted of different layers.

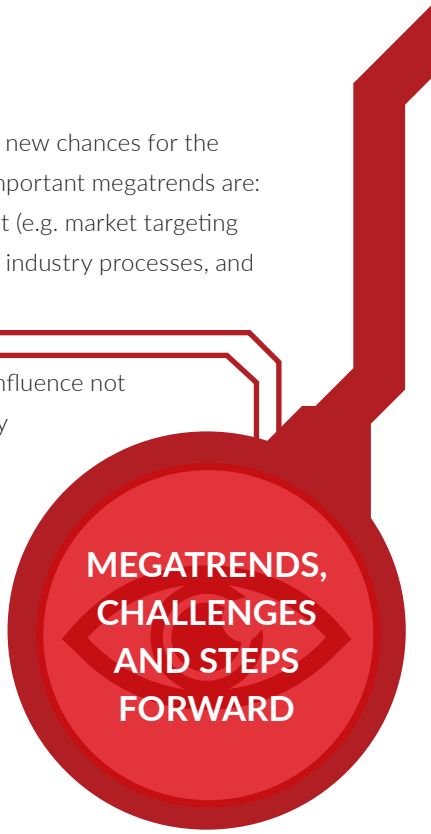
CYBERSECURITY ASPECTS

- Collaborative and adaptive multistakeholder approach is a basis of well-working Internet Governance. Dialogue between and co-operation of different stakeholders should apply also in the field of cybersecurity. All actors play significant roles in this area and, therefore, all stakeholders should be included: governments, civil society, technical community, academia and private sector. Each of them responsible for its own sector, but also co-operative with others.
- Continued development of security standards with input from all stakeholders will further improve cybersecurity efforts.
- Further participation in Internet Governance is needed from all stakeholders in developing countries, as well as from "weaker" stakeholders in developed countries that do not have sufficient representation or participation. They should be included in the processes in accordance with the principle of multistakeholder approach. The need for gender balance was also brought up.
- In the context of cybersecurity, especially the problems of intellectual property rights and human rights were underlined. It was recommended to look for practical recommendations related to the application of the existing laws and provisions in this area to cyberspace. Europe should be a champion in that.
- In order to accomplish a well working private public co-operation and information exchange, the need of trust was underlined. One way to achieve this is to gather actors and communities that share similar goals and values. Law enforcement co-operation and CERTs and co-operation within FIRST were given as examples.
- The need of exchanging serious lessons learnt between various stakeholders is needed as well as real coordination of actions as it is outlined in the draft NIS Directive. Examples of destructive attacks were given.
- Increasing cybersecurity capabilities globally was pointed out as the right direction.
- Further development and implementation of technical tools that increase security is needed. It can be achieved by supporting R&D and innovation.
- Usage of IP v.6 and DNSSEC was recommended. The interest for implementation should come from the business.

FUTURE STREAM

DIGITAL MEGATRENDS – CYBERSECURITY IMPERATIVES

Participants of the session identified a few main megatrends, which on the one hand will bring new chances for the society but on the other hand will pose new challenges that will need to be faced. The most important megatrends are: the development of IoT (which currently influences at least 14 industries), identity management (e.g. market targeting and personalisation), IP infringement, big data, bio/nano/quanto-computing, the automation of industry processes, and Smart Cities.



All digital trends come together and need to be thought about concurrently. Megatrends will influence not only functioning of people but also they will have impact on economy, public policies and many other areas. The most important implications pointed out during the session:

- Ontological shift – new reality, where concepts and solutions known from "analog" world, doesn't fit anymore to the digitalised environment. One manifestation of this situation is the fact, that majority of the traditional institutions are not able to hold the data which is in the hands of new clusters of interests. In order to face this problem more pragmatic regional cybernetics were advised by one participant.
- Privacy - important impact on citizens. The scope of the consequences can be realised by looking at some numbers: 90% of the data that exists today was generated in the last year. It was pointed out that privacy protection will require solid actions from governments' side, the other prediction is that megatrends (technologies) will eventually commit to our protection.
- New model of doing business and the change of the security paradigm. New value will be generated by information, analytics and data processes.
- Impact on prices – digitalisation will continue to have impact on workload and it can lead to bigger unemployment in blue-collar sectors and changes in salary structures.
- New global players will arise in the digital sphere and they will have increasing impact on international geopolitics.
- New social effects will occur like less transparent, algorithmic discrimination (in context of many aspects like pricing).
- Development of various forms of organised crime as well as further usage of Internet by terrorists were identified as crucial threats to cybersecurity.
- Cyberattacks pose a great threat to critical infrastructure, which is to large extent connected to the Internet and thus, it is more vulnerable to attacks. Benefits that come from automation of industry processes must come hand in hand with security measurements.
- Development of IoT will pose enquiries about liability. The question is who will be responsible for the possible problems. In context of liability, one participant underlined the need for creating market conditions for security, where entities responsible for the mishandling of the data would be punished.
- Cheap, untested technologies will pose significant challenge to the cybersecurity of IoT.

GENERAL REMARKS ON MEGATRENDS AND CYBER-SECURITY

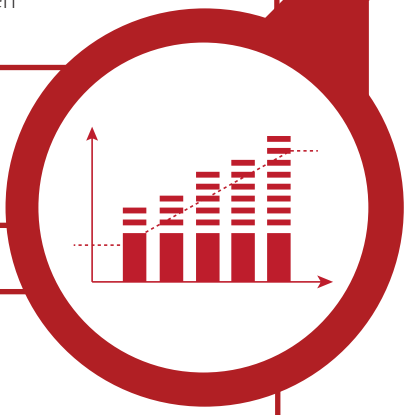
- Above-mentioned challenges must be overcome in order to uphold positive effects of megatrends. Despite the given challenges, one must remember that societies are empowered by new technologies.
- In practice, when securing IoT devices, their whole architecture ("full stack") must be taken into account: the hardware, the network, and the software layer. Each layer of the stack may be affected by different threats both external and internal to its function.
- In context of the regulations, two different standpoints occurred. The positive role of bottom-up, self-regulation processes (referring to PEGI example) was pointed out, however regulations are needed at least in more critical sectors. There was a strong statement in this context that the opposite of bad regulation is not no regulations; it is better regulation.
- One possible prediction for the future is reverse megatrends.
- Common denominator during the discussion was for a better education and greater awareness. A related risk is that in a world lacking the knowledge and education on the nature of 21st century economy and technological progress, the nascent IOT sector may be strangled in areas where an overemphasis on risk plays into populist political fears.
- The problem of outdated legislation was underlined. Two possible approaches were pointed out – one proposed solution was to create new clear rules in order to avoid difficult interpretation. Second approach propose rather to accept more flexible framework approach towards increasingly complex situations.
- One recommendation was to change paradigm of security in new business model – focus on proactive measures in the company and prepare as much as possible before the attack.
- Another recommendation was to create joint task forces also at the level of private and public organisations where specialists from various branches could work together in order to deal with cyberthreats.
- Finally the need for development of technology that will help to fight the threats and overcome challenges was underlined.

BUSINESS STREAM

NEW REGULATORY FRAMEWORK

- While talking about business involvement in providing cybersecurity, one remark has to be made. On the one hand, business has to be aware that its responsible behaviour to a very large extend determines overall level of public security. On the second hand, it has to be underlined that the basic role of private sector is to make effective business and create new effective business models in respect to existing or predictable legal framework.

- It was highlighted that business has to be socially responsible, however business may not take all of the risks. Therefore, it is very important to divide the risk in respect to providing security and trust between the state and private sectors.



- European regulations should provide legal confidence and harmonise the legal provisions in Members States.

- Positive effects of regulations cannot be undermined by the risk of overregulation. There is a danger that, in case of badly designed regulations, business will fulfil obligations only at minimum level in order to avoid sanctions. The legal tools will be effective only if businesses recognise their added value. Additionally, too heavy regulations may impose too much burden for smaller players.

- Regulations must provide inclusiveness of all stakeholders and cannot lead to building barriers among different players.

PRIVACY CONCERNS

- It was stressed that it is very important to find the right balance beetween security and privacy. But both terms are not opossite. It builts synergy because there is no privacy in unsafe envirnoment but, on the other hand, providing high level of privacy standards does not mean safety, as such.
- Privacy has to be provided on different levels: citizen – government and client – company.
- Discussion on the encryption has to be continuated especially in relation to the problem of both privacy and general security of the data.
- Big data profiling has to be seen as another area where responsible actions have to be provided.
- New business models should make the protection of personal data as an integral part of their service.
- More awareness and transparency is needed. It is necessary to effectively inform consumers and other personal data subjects about their rights and the scope of the data which is processed. People have to understand what happens with their data.
- Ongoing discussion about monetising the privacy should be continued and deepened. Awareness rising in context of this debate seems to be especially important.

CO-OPERATION

- Information sharing is seen as one of the most important elements which helps to provide cybersecurity. The crucial factor of success in this matter is bidirectional flow of the data – not only provided from business to public sector but also the other way around.
- Future challenges relate also to data breach notification to clients and to relevant public authorities. Responsible and efficient solutions in this matter should be discussed.

- Digital Single Market strategy is seen as a chance to make Europe more competitive.

- In context of DSM, a lack of neutrality of VAT (value added tax) and different rates in many states were pointed out as obstacles.

- There was a strong voice from the business representative that the scope of Network and Information Security (NIS) Directive is too wide and should be limited to critical infrastructure and to not apply to all service providers. One argument that supports this standpoint is that the broad scope of the Directive will increase the amount of data that would be processed and would have to be protected. This will be a challenge not only for private sector entities but also for public authorities.

BUSINESS STREAM

ROLE OF BUSINESS IN PROVIDING CYBERSECURITY

- Similarly to the previous sessions, there is no consensus on the need of imposing regulations on the market. Talking about potential challenges of this process business underlines fast changing environment, responsibility of private business and reactiveness of regulations. On the other hand, public sector points out that regulations and sanctions serve as framework conditions for the business actors and may function as an important incentive which will increase level of cybersecurity.

- Cybersecurity market cannot be fragmented. Regulations should lead to the harmonisation of the different approaches rather than impose very strict solutions on how particular tasks should be performed.

- For the purpose of using the same nomenclature, it is important to underline that there is a difference between standards and regulations. Moreover, different types of standards need to be differentiated. Standards, among others, play an important role in the area of interoperability which is the basis for innovation.

- There is a need for paradigm shift in the area of thinking about cybersecurity. A positive message should be promoted. Enterprises must not only think how much they can lose due to cyberthreats, but mostly how much they can save if they invest in cybersecurity. It will be helpful to present concrete figures to the CEO. Cybersecurity has to be understood as a business advantage rather than an unnecessary burden.

- European Union creates and promotes platforms of public-private co-operation (like NIS Platform, Public-Private Partnership on cybersecurity) which should increase innovation and cybersecurity. But the success of the actions will depend on implementation phase.

- Currently, tools and solutions that will help to enforce future and existing legislation are being developed. R&D programs in the area of risk management and privacy are crucial. Public entities, academia and private sector have to be involved in building these solutions as broad as possible.

- Special attention has to be paid to the SMEs which very often cannot afford to implement very advanced cybersecurity solutions and hire high qualified security professionals. In order to overcome the problem of smaller resources, SMEs may or use help from partners that specialise in the field of cybersecurity and offer proper tools and service. Also, they might want to develop their own capabilities – for that purposes there should be a possibility to apply for funds which should be specified and adjusted to their specific needs.

- The good example of giving support to SMEs is call for projects HORIZON2020: DS-02-2016: Cyber Security for SMEs, local public administration and Individuals which enable small entities with more difficult access to solutions in field of cybersecurity to introduce some innovative solutions.

- The experience of the Polish National Centre for Research and Development shows that, although there are both national and European funds for cybersecurity projects, not so many applications gain funds. There are a few factors that make the project successful: offered projects should meet the demand of the market, ready for commercialisation and most of all continuity of the project has to be provided.

- Plans and priorities for domestic and international funding projects should be established in the course of broad consultations with all the stakeholders – industry, public sector, civil society and academia.

- Very important elements of cybersecurity are innovation and creativity. Time is crucial in order to increase these two features. Therefore, while funding innovative projects, bureaucracy and paper work need to be reduced. Fast track for innovative solutions is a good solution.

- Start-ups play significant role in the area of cybersecurity, especially while looking for innovative solutions. Europe (EU and MS) has to support its own start-ups so they will not have to look for the funding in the US and they will stay in Europe. It will help to build intellectual capital in the region.

- The basis for the European Commission action in cybersecurity was established in the "Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace." The document develops five major actions aiming to foster the development of industrial and technological resources needed for the realisation of the Digital Single Market.

COMPREHENSIVE APPROACH – AWARENESS IS THE KEY

- While thinking about cybersecurity, entities have to remember about all components – technological aspects, process and people. In the context of people, the main focus should be on increasing knowledge. It was estimated by one of the participants that around 80-90% of cyberthreats could be reduced by implementing rather simple security measures resulting from raising the level of knowledge among Internet users.
- Greater awareness in the field of cybersecurity should create positive demands from ICT suppliers.
- In order to increase the level of knowledge and skills, more national and international European cyber competitions should be organised.
- Young people should be encouraged to pursue this career path.
- The lack of well-educated and prepared cybersecurity work force is one of the most burning problems. Governments have to prepare and implement strategies of education that will answer the needs of IT and, more specifically, the cybersecurity market. The board of the company must be also educated in terms of the cybersecurity issues.
- The biggest challenge is to inform customer about risks so they will use cyberspace more responsibly. In order to increase awareness more security awareness sessions and trainings are needed.
- Cybersecurity should be mainstreamed into communities which are not technologically advanced. One way to do it is to include security technologies in the products. It is important to provide people with simple, cheap and easy-to-use tools. It was recommended to move to automate certain security features (for instance auto-update).
- Private companies have to shift toward secure software development.
- Companies have to remember that upgrading internal, already existing human capabilities is an option.
- Cybersecurity has to be seen as a broad area of expertise - not a single specific expertise.
- While talking about the strategies that will help to build human resources, the Israel example should be examined. Good practices from that country may be adjusted and adapted to European reality. One general recommendation will be to adopt state mission where cybersecurity innovation is a priority. Therefore, each country should create a holistic ecosystem where all stakeholders co-operate in the field of cybersecurity innovation and where needed funds are secured.
- While thinking about cybersecurity, we should focus more on addressing threats - phases of detection and response should be emphasised.
- Open source tools can help to reduce threats.

COMBATING CYBERCRIME*

LEGISLATION

- Global scale of cybercrime requires effective international co-operation. The key is to provide international harmonisation of various legal systems. Budapest Convention on Cybercrime is a good tool in this context.
- KI: Signatories of the Budapest Convention has to promote its provisions in order to broaden its scope.
- Strong, comprehensive domestic legislation on cybercrime (both substantive law and procedural law) precisely adjusted to international standards has to be established.
- KI: Both international standards and domestic legislation have to be regularly updated.

CO-OPERATION

- Co-operation in terms of combating cybercrime is fundamental and should be based on multistakeholder approach.
- Co-operation has to take place on domestic and international levels and should involve law enforcement, private sector, civil society and academia.
- The co-operation has various forms (e.g. threat intelligence or best practice sharing) and has to be adjusted to different stakeholders involved. For instance, different business sectors have specific features and business models– this has to be taken into account while establishing co-operation.
- International co-operation has to be developed on various levels. Work of the agencies like EUROPOL is equally important to bilateral co-operation between national law enforcements. This aspect has to be enhanced.
- Information sharing (between various stakeholders) has to be based on previously established mechanisms.

* Recommendations have been prepared in co-operation with experts from the Polish Platform for Homeland Security (PPBW). PPBW was established as a forum for dialogue between the end users, the research and the development organisations as well as the administration responsible for financing of research. With time, the PPBW has also become a platform for formation of consortia with the aim to develop dedicated technological and IT solutions to support the operations of entities for public security. It is also actively involved in legislative work aiming to develop appriopriate laws that enable implementation of modern technologies developed during research and development projects. Moreover, by providing consulting and educational services, PPBW supports the process of building public trust in the new security technologies.

CAPACITY BUILDING

- There is an urgent need to build national and international capabil ities to sufficiently combat cybercrime and to to constantly revise them.
- Training and skills development system for judiciary and law enforcement has to be in place, so that these entities are able to fulfil their duties in the new cyberenvironment. For instance, judiciary has to possess skills and knowledge on how to process digital evidences, and law enforcement has to be familiar with digital forensic analyses and cyberinvestigations. Providing this will allow to create a system of cyberspecialists both within judiciary and law enforcement.
- KI: Specialised cybercrime police units has to be established and be given access to the most innovative tools which will support their work.
- KI: Broadly understood capacity building has to be supported by the state (also financially).
- KI: More advanced countries should support others in capacity building efforts in order to increase overall level of cybersecurity.
- KI: Building capabilities has to be conducted in line with awareness rising campaigns.

PRIVATE ENTITIES

- Private entities are primarily self-responsible for their cyberprotection. Nevertheless, state should actively support their efforts.
- While building cyber capabilities within private entities, technical, procedural and organisational aspects have to be taken into account. It is advised to resign from the security models based purely on defence in depth. This so-called “castle approach” should be enriched by more proactive approach with strong elements of, among others, investigation activities which would, for instance, allow threat intelligence sharing.
- KI: While talking about information sharing, private entities (especially ISPs) play crucial role and have to be encouraged to co-operate. A role of private entities (especially ISPs) is crucial in the concept of information sharing and, therefore, they have to be encouraged to co-operate with other stakeholders.

CYBERSEC 2015

IN NUMBERS

CONFERENCE

1
Emerging Public Policy Challenge

4
Thematic Streams

6
Discussion Panels

8
Breakout Sessions

TIME

13
Months of Preparations

16
Hours of Simultaneous Interpretation

20
Hours of Networking Opportunities
forge new professional contacts

OPINION

of participants were satisfied with their overall experience

of participants were delighted with the conference venue - ICE Krakow Congress Centre

of participants would recommend attending to a collegue

PEOPLE

> 45
Accredited Journalists

>80
People from the CYBERSEC's Team

130
Speakers

>400
Participants representing 20 countries from Europe and U.S.

MEDIA & MEETINGS

>60
Interviews for CYBERSEC TV

1800
Photos

2700
Cups of Coffee

77500
Impressions on Twitter

CYBERSEC 2015 PARTNERS

CONTENT PARTNERS

POLISH PLATFORM FOR HOMELAND SECURITY

EY Building a better working world

PARTNERS

Bank Polski

PZU Z myślą o bezpieczeństwie

BalaBit IT Security

HONORARY PATRONS

Republic of Poland Minister of Foreign Affairs

MSP Ministerstwo Skarbu Państwa | Ministry of Treasury Republic of Poland

Ministerstwo Administracji i Cyfryzacji

BBN National Security Bureau

UKE Office of Electronic Communications

KRAKÓW krakow.pl

Małopolska KRAKÓW Region

eer European Entrepreneurial Region

PATRONS

NIK

Military University of Technology

RCB Rządowe Centrum Bezpieczeństwa

Komisja Nadzoru Finansowego

JAGIELLONIAN UNIVERSITY IN KRAKÓW

Politechnika Wrocławska

e-COMMERCE POLSKA IZBA GOSPODARKI ELEKTRONICZNEJ

MEDIA PATRONS

TVP INFO

RZECZPOSPOLITA

wSIECI

wGospodarce.pl

polska-zbrojna.pl

BIZNES ALERT

CIRE.PL Centrum Informacji o Rynku Energii

Defence24

wnp.pl

NOWY PRZEMYSŁ

NIEBEZPIECZNIK.PL

kierunekchemia.pl

EurActiv

WWW.KRAKOW.PL

CONFIDENCE

WKB law firm was involved in preparation of the recommendations.

CO-FINANCED BY

NATO OTAN

Ministry of Foreign Affairs Republic of Poland

Consulate of the United States of America

STRATEGIC PARTNERS

Microsoft

CISCO

EXATEL

people behind technology

PGZ

PARTNERS & CO-ORGANISERS

KRAKÓW krakow.pl

KRAKOW convention bureau

MAIN PARTNERS

FireEye

FIDELIS CYBERSECURITY

FORTINET

KGHM POLSKA MIEDŹ

BGK BANK GOSPODARSTWA KRAJOWEGO

PERN „Przyjaźń" S.A.

Enea

ORGANISER

THE KOSCIUSZKO INSTITUTE

CO-ORGANISER

cybersecurity FOUNDATION

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES

POLICY REVIEWS

OPINIONS

CONTRIBUTE TO THE NEXT ISSUE!
CALL FOR PAPERS:
EDITOR@CYBERSECFORUM.EU

THE KOSCIUSZKO INSTITUTE

WWW.CYBERSECFORUM.EU

EUROPEAN CYBERSECURITY FORUM

Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

26-27 September 2016, Kraków, Poland

CYBERSEC 2016

STAY TUNED

WWW.CYBERSECFORUM.EU