

EUROPEAN CYBERSECURITY FORUM

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

26-27 SEPTEMBER 2016 - KRAKÓW, POLAND

VENUE: ICE Kraków Congress Centre



CYBERSEC EU 2016 CONFERENCE PROSPECTUS



STATE
STREAM



MILITARY
STREAM



FUTURE
STREAM



BUSINESS
STREAM

WWW.CYBERSECFORUM.EU

CYBERSEC - OUR MISSION

Our mission is to support and facilitate the development of strategic, cybersecurity-focused decisions for Europe.

Our goal is to build a dedicated platform for co-operation among government representatives, non-governmental organisations, and key private-sector organisations.

WHAT IS CYBERSEC?

The **CYBERSEC** Forum is the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe.

We promote practical recommendations that increase resilience to cyberthreats, at both micro and macro levels (specific economic sectors, countries, EU as a whole).

Through dialogue oriented and targeted approach to specific challenges, we provide a strong cross-stakeholder impulse for increased awareness and urgency in developing solutions that reach beyond national borders and enhance collaborative efforts.

In particular, our recommendations help strengthen co-operation between the Visegrad Group, the Baltic Countries and other countries of Central Europe.




WHY CYBERSEC?

The key aspects of social, economic, and military interactions are being increasingly transferred to cyberspace. The benefits for business and the functioning of states are obvious. However, this increasing dependence on ICT, necessitates the development of a cybersecurity system that involves all stakeholders and puts cybersecurity education in the centre of the debate. This is increasingly becoming a precondition for economic growth, socio-economic stability, and international security.

Many countries, therefore, are making even more significant strides in turning their attention to cybersecurity and building their defensive and offensive capabilities in cyberspace. However, this is only the beginning of a long road, on which dialogue, co-operation, and best-practice sharing, are only few of the necessary steps.

WHY NOW?

Incidents in cyberspace are an everyday occurrence. Many of them have important consequences in “the real world”. Cyberattacks on critical infrastructure threaten the security of states and millions of citizens. The private sector, which is increasingly becoming the direct or indirect target of attacks, bears huge economic losses. In the meantime, geopolitical tensions continue to rise at an alarming pace.



**THE BUILDING AND STRENGTHENING
OF CYBERSECURITY SYSTEMS,
THEREFORE, MUST BE THE SUBJECT
OF A COMPLEX ANALYSIS AND DEBATE
RIGHT NOW.**

**AT A CHALLENGING TIME FOR EUROPE,
CYBERSEC ADDRESSES A VERY
IMPORTANT GAP IN THE CALENDAR
OF THE MOST INFLUENTIAL EVENTS
AND CONFERENCES DEDICATED TO
THE STRATEGIC PROBLEMS
OF CYBERSECURITY IN EUROPE.**

WHY EUROPE?

Intense geopolitical tensions, extensive usage of ICT systems by terrorist organisations and more frequent and serious-in-consequences attacks on critical infrastructure, create the need for Europe to build a comprehensive cybersecurity system. Such a system will need to rely on more efficient forms of co-operation between public and private sectors, as well as educating experts for the European market of innovative cybersecurity products and services.

Finally, 2016 sees the early stages of implementation for important legislation, reorganising European legal order in several aspects of cybersecurity.

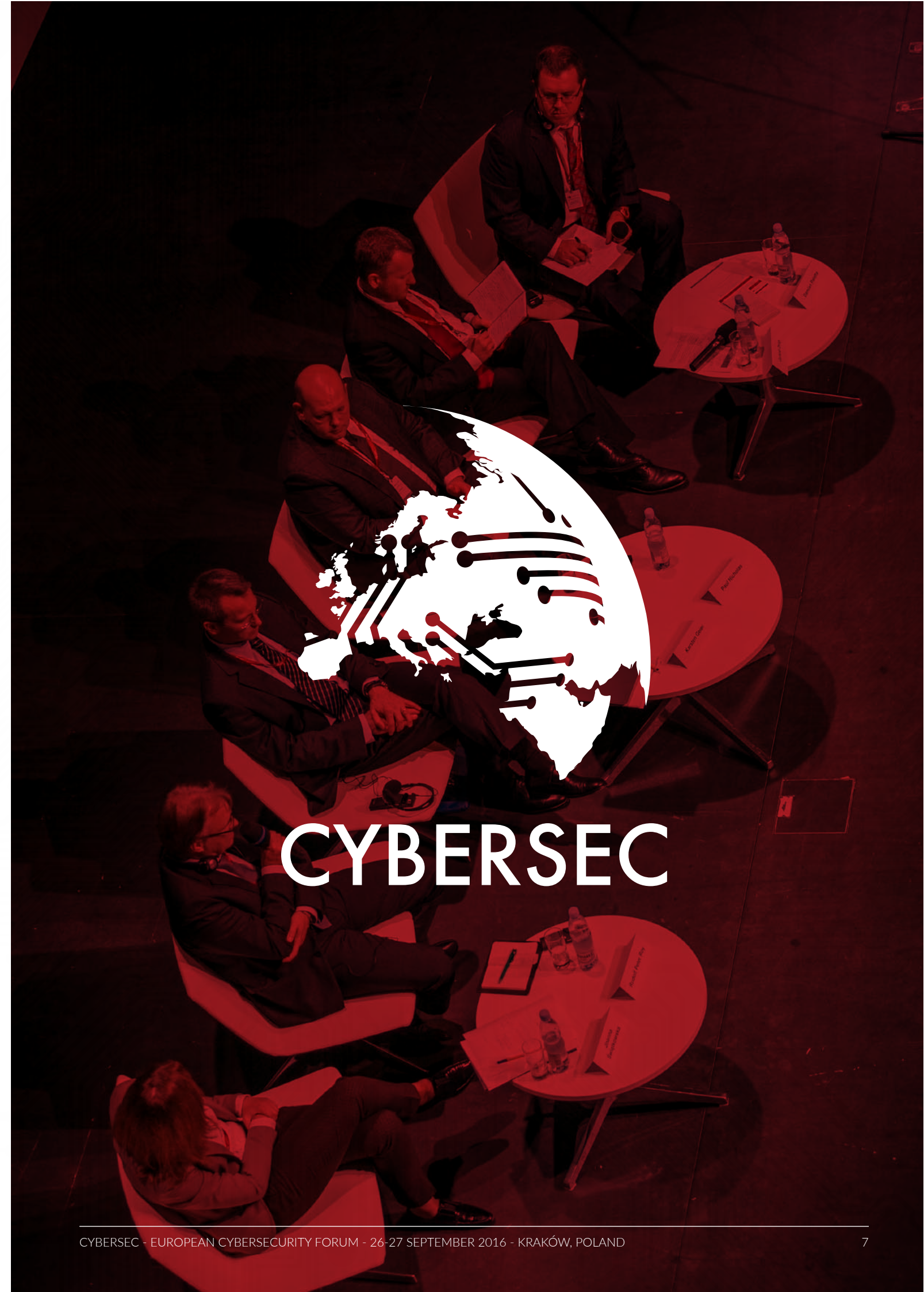
WHY FOCUS ON THE EURO-ATLANTIC DIMENSION?

Strategic approaches to personal data security, privacy and cyberspace sovereignty among the partners of the transatlantic alliance have been following increasingly divergent paths. In the wake of emerging threats, dialogue and enhanced co-operation are now essential for partners in order to strengthen mutual trust and develop common cyberspace policies. This new path is of paramount importance for international security and peace.

WHY POLAND?

CYBERSEC will be held in Poland, the country which, due to its geopolitical position, is particularly exposed to destabilising activities conducted in cyberspace. As Poland is one of the largest EU Member States, hence, a key actor in Central Europe, its role in setting the agenda will have a significant impact on the new cybersecurity roadmap extending far beyond the region.

Poland will host the 2016 NATO Summit in Warsaw, with issues concerning cybersecurity on top of the agenda of this strategic meeting.



FOUR THEMATIC STREAMS CONCERNING KEY CYBERSECURITY ISSUES



STATE STREAM

Facilitating strategic cross-stakeholder co-operation, the development and implementation of the most important public policies for digitisation and cybersecurity.



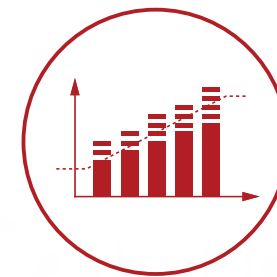
FUTURE STREAM

Providing structured support in the process of identifying trends, challenges and opportunities for both the ICT sector and the global information society and contributing to cybersecurity innovations.



MILITARY STREAM

Addressing the evolving dimensions of cyberconflicts in Europe, the role of NATO and the need for comprehensive military co-operation.



BUSINESS STREAM

Exploring the various roles of the private sector in conducting joint initiatives, crafting regulatory frameworks and developing mature cybersecurity markets

STATE STREAM

The notion of increased connectivity and the growing, technological complexity of our daily lives, translate directly to specific challenges for the state. Therefore, it is essential for individual states to seek to adopt public policies that reflect these new realities. Arguably, states and international institutions should define a new approach to cyberspace at large. Merely redefining the current policies will not be enough. A responsible approach to cybersecurity demands a new, solid foundation that will continuously strengthen cyber resilience, both under the current and the future conditions.

Close international and private-public co-operation must be propagated. In the twenty-first century, governments will increasingly seek to harness the power of cyberspace to implement their internal and external policies. Hence, there is a great need for strengthening international relations, credibility and co-operative networks.

BREAKOUT SESSION 1

CO-OPERATION IN THE CEE TOWARDS
SUB-REGIONAL CYBERSECURITY
- DEVELOPING CONFIDENCE
BUILDING MEASURES

DISCUSSION OBJECTIVES:

- To disseminate the concept of CBMs for cyberspace
- To identify and promote measures that could complement international/regional CBM processes from the perspective of the CEE region and for the benefit of the countries from the region
- To identify additional instruments for the CEE region designed to enhance co-operation and transparency in the field of cybersecurity on the national and sub-regional level

BREAKOUT SESSION 2

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

DISCUSSION OBJECTIVES:

- To identify the main challenges of NIS Directive implementation
- To develop recommendations for NIS Directive with reference to implementation roadmap
- To harmonise Member States strategies and actions in the field of cybersecurity



STATE STREAM

MILITARY STREAM

Cyberspace is an immanent dimension of today's military conflicts. Governments and international organisations are currently facing the challenge of developing new, end-to-end strategies and defence doctrines that take into account this new perspective.

Given that military cyber-operations are very different from conventional warfare, the principles governing them must be carefully considered, while taking into account the experience of entities operating in various areas of cyberspace. The modern digital battlefield not only opens up new possibilities for carrying out military operations but also presents challenges from new security threats.

BREAKOUT SESSION 1

NATO CYBERDEFENCE POLICY AFTER THE WARSAW SUMMIT

DISCUSSION OBJECTIVES:

- To discuss and promote conclusions of the NATO Warsaw Summit
- To explore the untapped opportunities for the enhanced NATO-EU cyber co-operation
- To identify the next steps for NATO's cyberdefence policies

BREAKOUT SESSION 2

FIGHTING TERRORISTS WITH TARGETED CYBER-TOOLS

DISCUSSION OBJECTIVES:

- To analyse different strategies for utilising cyberspace for achieving planned goals
- To identify and discuss the various activities conducted in cyberspace that can help to fight terrorist groups (with a special focus on cyber intelligence activities)
- To discuss the possible controversies related to cyber operations aimed against terrorists.



MILITARY STREAM

FUTURE STREAM

The dynamic development of cyberspace has an increasingly powerful influence on societies, political developments and economic prospects. An effective global network would not only benefit from information-sharing, new products and services, but would also help highlights the real security threats for new communication technologies, privacy and data protection.

In order to embrace future challenges, the international community should speak in one voice during the process of identifying and addressing the various, complex and diverse trends of the evolving cyberspace. This will allow for creating strategies, designing concepts and ideas that are instrumental in the context of the expected challenges, especially in cyber and IT education, establishing centres of cyber excellence as well as cybersecurity hubs. The functioning of states, societies and economic entities will depend on the results of these findings and actions.

BREAKOUT SESSION 1

PREPARING THE WORKFORCE FOR THE UPCOMING CYBER CHALLENGES

DISCUSSION OBJECTIVES:

- To identify specific areas of expertise where cyber specialists are most in demand
- To create strategies for education and training (the human resources gap).
- To identify the role of states, EU, NATO, the private sector and the academia

BREAKOUT SESSION 2

CYBERSECURITY INNOVATIONS - FOSTERING DEVELOPMENT AND CO-OPERATION

DISCUSSION OBJECTIVES:

- To explore the best practices in building multi-stakeholder communities where the most creative ideas and the most innovative R&D projects are given proportionate emphasis
- To identify the factors that boost innovation in the field of cybersecurity
- To enhance co-operation and networking opportunities between various cyber communities



FUTURE STREAM

BUSINESS STREAM

The dynamic development of cyberspace has created completely new opportunities for businesses. At the same time, companies become targets of cyberattacks launched from anywhere across the globe. Cyberattacks may result in the disruption of various business processes and services. They may also lead to the physical destruction of infrastructure, loss of confidential information, financial resources and, last but not least, damage to business reputation. It means that cybersecurity must be treated as an intrinsic aspect of the overall business strategy.

Furthermore, the private sector is constantly engaged in the development of mature cybersecurity solutions. The role of the private-sector companies in enhancing the overall level of national security grows every day. Private-public co-operation is the key foundation for all successful actions, projects and initiatives. Hence, it must be treated as the central component of national cybersecurity strategies.

BREAKOUT SESSION 1

CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS

DISCUSSION OBJECTIVES:

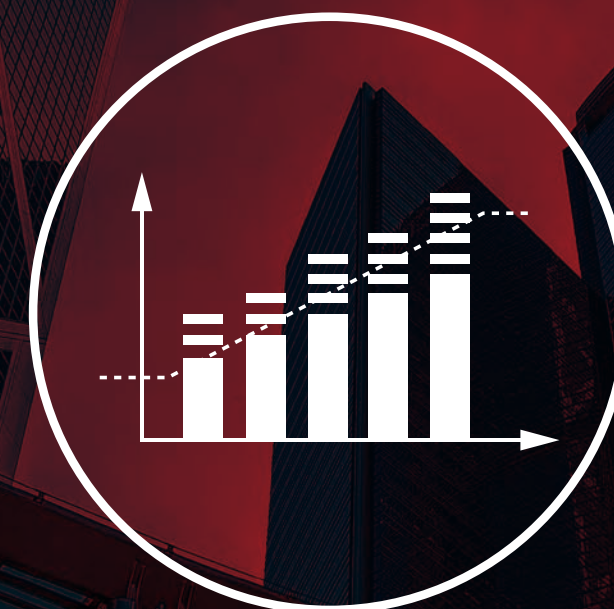
- To understand the importance of industrial control systems (ICSs) and specific conditions that impact cybersecurity
- To identify the main cyberthreats that potentially threaten the security of ICSs
- To develop security recommendations for ICS (in different sectors)

BREAKOUT SESSION 2

GLOBAL, REGIONAL AND NATIONAL PUBLIC-PRIVATE CO-OPERATION – SUCCESS STORIES

DISCUSSION OBJECTIVES:

- To identify the common denominators of successful private-public initiative
- To explore the various strategies aimed at bringing together both the public and the private sector in the process of designing cybersecurity eco-systems and jointly responding to cyberthreats
- To promote valuable initiatives and enhance co-operation between stakeholders.



BUSINESS STREAM

THE CYBERSEC FORMULA

CYBERSEC boasts a comprehensive conference programme designed to tackle timely, real problems. **CYBERSEC** agenda is continuously being developed and improved in co-operation with partners from the public, non-governmental and commercial sectors

Two days of thought-provoking debates in a variety of innovative formats involve key cyberspace stakeholders. Through moderated dialogue, we exchange ideas on strategic issues concerning cyberspace and digitisation, put the key challenges of cybersecurity to

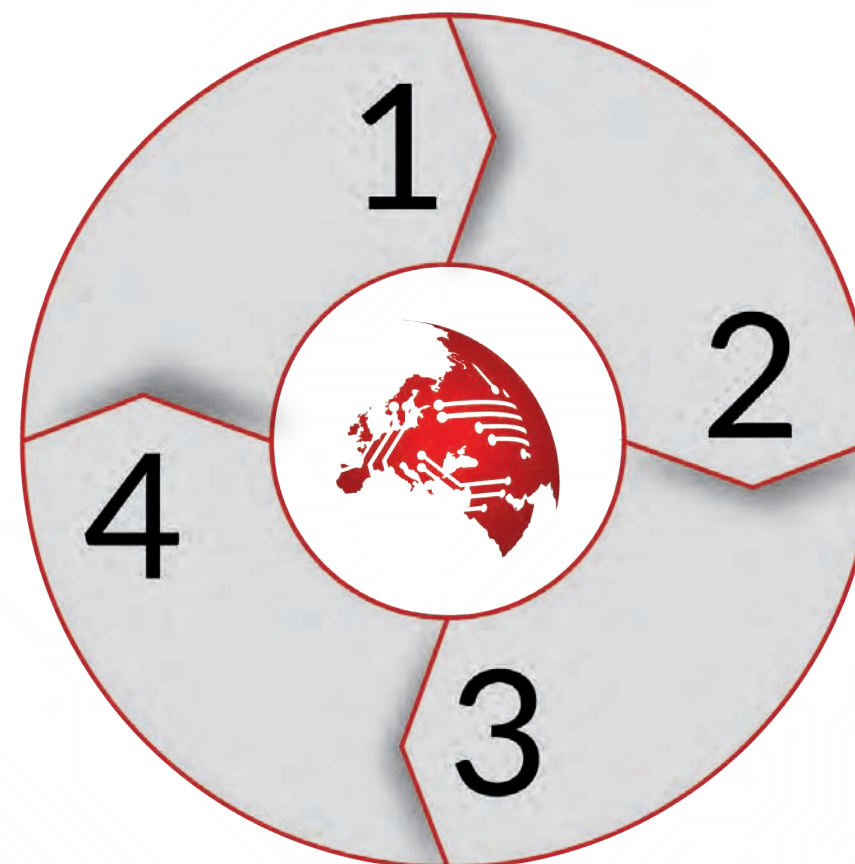
scrutiny and assessment from high-level perspective. Our experts steer the discussions towards specific regulatory solutions for the EU and individual Member States. Our formula includes a series of joint, follow-up activities and recommendations within four thematic streams - State, Military, Future and Business. Last but not least, networking and building relationships are always part of our design process.

PROBLEM IDENTIFICATION preparation stage

*WEBINARS preparing BREAKOUT Sessions
for STATE, MILITARY, FUTURE
and BUSINESS streams*

MONITORING THE EXECUTION OF RECOMMENDATIONS post-conference stage

*RECOMMENDATIONS
PROMOTION - MONITORING*



BRAINSTORMING AND SEARCH FOR SOLUTIONS CYBERSEC AT WORK

*DAY 1 - KEYNOTE Presentations - BREAKOUT Sessions
DAY 2 - PANEL Discussions*

RECOMMENDATIONS final stage

*BUILDING RECOMMENDATIONS
from DAY 1 and DAY 2 - FINAL REPORT*

AN INNOVATIVE FORMULA FOR DEBATE RESULTING IN TARGETED RECOMMENDATIONS

PROBLEM IDENTIFICATION

The choice of expert Stream leaders – representatives of the public and business world as well as partners who identify (in the course of webinars preceding the **CYBERSEC** Forum) the key cybersecurity issues to be examined during the Breakout Sessions and discussion panels within each Stream.

BRAINSTORMING AND LOOKING FOR SOLUTIONS

The format of all the discussions and events will be implemented with a view to guide the development of solutions to specific, pre-defined problems. The main conference formats include the following:

- Keynote Presentations given by world-class experts, outlining the most important challenges facing each thematic Stream.
- Breakout Sessions (two BSs within each of the four Streams) – top experts from key domains will develop solutions to cybersecurity concerns based on in-depth analysis of cybersecurity problems.
- Discussion Panels: solutions from the Breakout Sessions will be presented by expert Stream leaders for discussion before decision-makers within the four Discussion Panels. This part will also constitute a summary of outcomes from all four Streams.

RECOMMENDATIONS

The final recommendations resulting from all **CYBERSEC** 2016 debates, will be gathered and shared via **CYBERSEC** platforms and websites of our institutional partners. The document will contain proposals of concrete initiatives and legislative solutions that can be implemented in individual states and across the EU, to increase cybersecurity across the continent.



MONITORING THE IMPLEMENTATION OF RECOMMENDATIONS

The implementation of **CYBERSEC** 2016 final recommendations will be systematically monitored. **CYBERSEC** organisers and Stream leaders will be in close contact with the addressees of the recommendations and will follow up on the implementation status.

SPECIAL SESSIONS

CYBERSEC 2016 will incorporate many more innovative dialogue formats. It will provide you with creative opportunities to explore the most pressing cybersecurity issues, but also it will allow you to build strategic relations and networks.

This year the issue of combating cybercrime will be one of the main topics discussed during our special sessions. Within this thematic framework we will particularly work on recommendations how to enhance cross-stakeholder cooperation in order to fight cybercrime more effectively.

CYBERSEC AT WORK ...AND AFTER HOURS

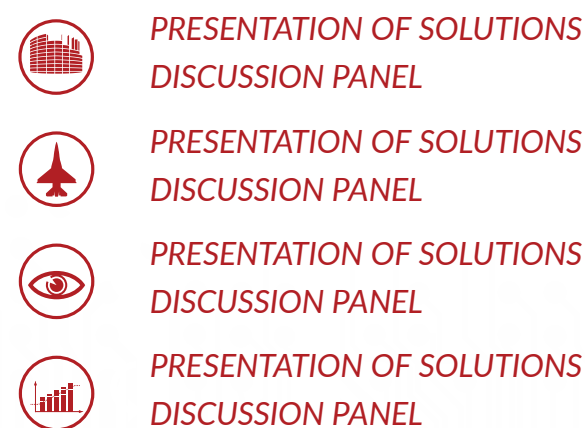
PREPARATION STAGE



DAY 1



DAY 2



RECOMMENDATIONS



Informal **CYBERSEC** evening events for forging relationships and casually exchanging ideas in picturesque surroundings.

- Banquet at the ICE Congress Centre.
- Gala Reception for invited guests in the "Wieliczka" Salt Mine



CYBERSEC GUESTS

CYBERSEC attracts senior representatives of governments from EU Member States, US and leading international organisations. We establish co-operation with European and globally-acclaimed cybersecurity experts and practitioners.

The list of participants also includes key private-sector representatives:

- 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
- Military & MoD Officials
- Internat. Organisations Reps.
- ICT
- Power Generation & Distribution
- Transportation
- Critical Infrastructure
- Defense & Security
- Finance & insurance
- Chemical Industries
- Mining & Petroleum
- Public Utilities
- Data Privacy
- CyberSecurity
- Manufacturing & Automotive
- Pharmaceutical

FROM THE FOLLOWING SECTORS

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



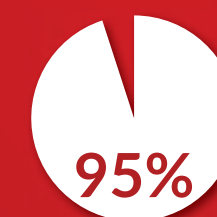
20

Hours of Networking Opportunities
forge new professional contacts

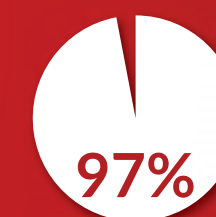
OPINION



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 colleague

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

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 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.

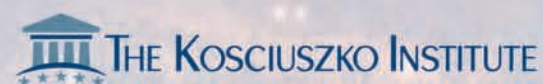
Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

 INSTYTUTKOSCIUSZKI

 @IKOSCIUSZKI



is the organiser of



CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

WWW.CYBERSECFORUM.EU



CYBERSEC

EUROPEAN CYBERSECURITY FORUM

Organising Committee
www.cybersecforum.eu
TT: CYBERSECEU
FB: cyberseceu
office: +48 12 632 97 24
cybersec@cybersecforum.eu

ul. Feldmana 4/9-10
31-130 Kraków

Chair of the CYBERSEC Organising Committee, Izabela Albrycht

CYBERSEC Programme Director, Joanna Świątkowska

