CYBERSEC
EXPO & FORUM

CYBERSEC EXPO & FORUM
19-20 JUNE 2024
PANEL DISCUSSION, 10:45-11:45
SOC NETWORKS
– EUROPE'S CYBERSECURITY SHIELD

SUMMARY CYBERSEC CEE EXPO & FORUM 2024

MAŁOPOLSKA
MAIN PARTNER

Kraków
HOST CITY

CYBERSEC EXPO & FORUM
19-20 JUNE 2024
MAŁOPOLSKA
MAIN PARTNER
CYBERSEC EXPO & FORUM
PANEL DISCUSSION, 10:30-11:30
WIRED FOR SUCCESS? EMPOWERING EUROPE'S DIGITAL INFRASTRUCTURE
dr Joanna Kulesza
Lise Fuhr
Ingrida Taurina
Marc Vancoppenolle
Host: Tomasz Piekarz
NCC-PL
Krajowe Centrum Kompetencji
Cyberbe[illegible]stwa

Kraków

wide

open

for

meetings

Kraków: when can we expect you?

A business event in a state-of-the-art facility, in a city boasting a thousand years of history all around you? The "wow" effect guaranteed! However, the MICE industry is not only about spectacular settings – it is also about professional organisation, state-of-the-art technology, comfortable accommodation and, last but not least, a range of leisure activities. Kraków offers all these – and much more.

The former capital of Poland, located in the southern part of the country, successfully combines the contemporary challenges with its centuries-old heritage. Woven into the historic fabric of the city, its infrastructure dedicated to events impresses with its modern design and functionality. It allows to organise a wide variety of events: trade fairs, conferences, congresses, symposia, and business meetings, all of them having top quality as the common denominator.

Venues such as the TAURON Arena Kraków, the EXPO Kraków International Trade Fair and Congress Centre, the CKF_13 Fabryczna Conference Centre, and the ICE Kraków Congress Centre can host events for thousands of participants as well as more intimate ones.

It is ICE Kraków that will be the venue of the 6th Cities Forum 2025, one of the most important events devoted to the development of European cities, with participation of 800 delegates from all around the EU. To host the Forum, Kraków had to outcompete 13 other European cities. The event will provide an opportunity to discuss cohesion policy, sustainable development, and metropolitan policies.

In the city, event organisers can count on the support of Kraków Convention Bureau.

The city's extensive range of hotels and their accessibility is an important asset: more than 12,500 rooms in almost 190 hotels, many of which of boutique type. The city also boasts air links to all major European cities. Kraków is a perfect destination for enthusiasts of active leisure and wellness, aficionados of culture and art, and also foodies – there is something for everyone here, and the only regret you may have is that you have spent too little time here.

MAŁOPOLSKA

MAIN PARTNER

Thanks to its openness to investments and innovation in the scientific, business, and local government sectors, the Małopolska Voivodeship demonstrates broad activity, cooperating with each of these sectors. Numerous programs and initiatives are being implemented in Małopolska that support the region's development and enhance its competitiveness not only in Poland but also on the international stage.

SUPPORT FOR THE PRIVATE SECTOR AND ENTREPRENEURSHIPS IN THE REGION

The #StartUP Małopolska acceleration program, launched in 2017, supports young entrepreneurs through several-month-long support programs, specialized workshops, and training sessions. The Małopolska Voivodeship also recognizes the potential of the startup community and supports the organization of technological events through the program "Małopolska – where technology becomes business". So far, around 190 initiatives have received support, involving approximately 110,000 people. The Centre Business in Małopolska (CeBiM), established by the Marshal's Office, Kraków Technology Park, and the Małopolska Regional Development Agency, offers an integrated system for servicing investors and exporters. CeBiM also supports Ukrainian companies that have relocated their operations to Małopolska, focusing on information, advisory, and networking services. Małopolska has been recognized as the European Entrepreneurial Region 2024, which shows international recognition and places the region in a high position regarding support, obtaining grants, and cooperation in Europe.

INTERNATIONAL COOPERATION

Małopolska actively participates in international economic cooperation, including with Ukraine, supporting the rebuilding and strengthening of entrepreneurship. In 2023, an economic mission to Lviv was organized, involving representatives of local government, Kraków universities, and clusters from Małopolska. As part of international cooperation, projects are being carried out with Kraków academic and scientific institutes, which increases Małopolska's potential on the international stage.

CYBERSECURITY

The Małopolska Voivodeship is actively working to enhance cybersecurity. Many initiatives aimed at increasing cybersecurity are conducted within the office, although there is no formally designated unit for this issue. Actions are carried out within various projects and by different departments, including through the Małopolska Council for the Information Society, which helps raise awareness and skills in defending against digital threats. Małopolska collaborates with institutions such as CERT (Computer Emergency Response Team), NASK (Research and Academic Computer Network), and the Police, allowing for a multi-faceted approach to cybersecurity management. The Małopolska Voivodeship runs numerous educational programs aimed at the region's residents, such as the "Internet Week" campaign and workshops on safe internet usage. Internal training sessions are conducted within the office, along with projects like "Safe Office" and "Cybersecure Local Government," supported by the "Digital Province" grant. The Małopolska Voivodeship was also the Main Partner of this year's European Cybersecurity Forum CYBERSEC 2024, which serves as a platform for discussion and knowledge exchange on key programs related to cybersecurity and digital transformation.

00:01:31
security
magazine
0,5
1
2×
5

Dear Readers,

The 19th edition of CYBERSEC has come to an end. This year, our event made its long-awaited return to Krakow, the birthplace of its co-organizers – the Kosciuszko Institute and the #CyberMadeInPoland cluster. Returning to the City of Kings and the Malopolska region has reinvigorated us, allowing us to tackle the challenges of cyberspace with renewed energy and to further develop our flagship project.

Since 2015, CYBERSEC has been a hub for exchanging views on the most pressing and dangerous cybersecurity threats, with participants from the public sector, business, academia, and non-governmental organizations. This year, our FORUM stage agenda focused on the theme **"BEYOND DEFENCE – TOWARDS PROACTIVE CYBERSECURITY”**. Through this theme, we aimed to highlight the importance of proactive and preemptive measures in cyberspace. As digital threats evolve, there is a need for a change in approach – proactive actions that involve strategic decisions, collaboration beyond traditional frameworks, CTI sharing and the implementation of modern technological solutions. Nations, businesses, and even individual internet users must now protect themselves in ways that anticipate threats and effectively counteract them before incidents occur.

A significant portion of the discussions, both on stage and behind the scenes, also centered on Poland's upcoming Presidency of the Council of the European Union in the beginning of 2025. Poland is preparing a set of ambitious and impactful digital priorities to advance during its term. The Kosciuszko Institute, along with this year's strategic partner—the European Cyber Security Organisation (ECSO) – signed a Letter of Intent to support the goals of Polish diplomacy, with backing from the Deputy Prime Minister and Minister of Digital Affairs of Poland, Krzysztof Gawkowski. The partnership will involve close engagement with the European cybersecurity ecosystem, including ECSO members and relevant stakeholders. This initiative aims to produce actionable recommendations and strategies that will contribute to a more secure digital environment across Europe.

CYBERSEC is not just a conference; it is also the most important EXPO in the region, aimed at developing and strengthening the cybersecurity market potential in Central and Eastern Europe. Held under the leitmotif **"BRIDGING EUROPEAN CYBERSECURITY MARKETS"**, it has once again become the place for everyone who wants to explore solutions, products, and companies in the field of cybersecurity, where exhibitors meet potential clients and build relationships. CYBERSEC collaborates with key organizations that bring together business and technical communities, stimulating innovation and generating new ideas through meetings with potential partners and collaborators. Additionally, it is where companies can meet investors, and investors can discover promising opportunities.

This year's edition welcomed 126 Patrons, Partners, Institutional Partnerships, Media Partnerships and Exhibitors, over a hundred Speakers, and thousands of Participants. On behalf of the entire CYBERSEC team, I would like to thank you all. CYBERSEC couldn’t happen without you, and we hope to see you again next year, during the 20th, anniversary edition of the European Cybersecurity Forum – CYBERSEC.

Maciej Góra, Project Manager
CYBERSEC Team

FORUM STAGE, 19 JUNE

WELCOME TO CYBERSEC

In her opening speech, **Marietta Gieroń, Chairwoman of the Programme Committee of CYBERSEC** highlighted the growing global challenges in cyberspace, particularly in the context of 2024's worldwide elections, emphasising the influence of cyber activities on voter behaviour and the increasing threats from nation-state actors and profit-driven hackers engaging in destructive attacks, espionage, and disinformation. Despite these challenges, Ms Gieroń noted the promising opportunities for cooperation in cyberspace, fostering prosperity and innovation, and encouraged participants at CYBERSEC to forge alliances and share insights. Emphasising CYBERSEC's role in building collective security, the speaker acknowledged the support from the Ministry of Digital Affairs of Poland and expressed hopes for realizing Poland's digital ambitions during its upcoming EU presidency. Next, **Łukasz Sęk, Deputy Mayor of Krakow**, took the floor to welcome all the participants of the conference. He emphasized the urgency and importance of cybersecurity, particularly in light of the growing impact of digital threats with the advent of AI and the ongoing war in Ukraine. Mr Sęk expressed his hope for fruitful discussions and proceedings throughout the conference.

TRANSFORMING POLAND INTO A DIGITAL POWERHOUSE

The opening keynote speech was delivered by **Krzysztof Gawkowski, Deputy Prime Minister and Minister of Digital Affairs of Poland**. At the outset, the Deputy Prime Minister expressed his hope that digital transformation could position Poland among the leading digital nations in Europe. He emphasized that digitalisation is an immensely responsible undertaking, affecting all aspects of social and economic life.

Mr Gawkowski highlighted the significance of cybersecurity for national security. He pointed out that Poland records 1,000 to 2,000 incidents daily, marking a year-over-year increase of 100%. The Deputy Prime Minister stated that the government's duty in digitalisation is to reduce silos, emphasising the need for interoperability and consolidated decision-making in strategic aspects of cybersecurity management. He also highlighted the importance of balancing the public and private sectors, underscoring that the government's priority is fostering business growth alongside efficient public administration, including reducing administrative burdens for digital economy entities.

For the first time publicly, Deputy Prime Minister Gawkowski announced that the government plans to allocate approximately 30 billion PLN from the Krajowy Plan Odbudowy (National Recovery Plan) towards the digital transformation of enterprises over the coming years, encouraging participation in multi-sector consultations on the expenditure plans. He then turned to the development of digital education and services, noting the continuation of successful projects from successive Polish administrations, such as mObywatel.

Mr Gawkowski also addressed the digital „cold war" between the West and Russia and Belarus, indicating that Poland aims to lead in shaping policies at the European level. He emphasised the crucial importance of dual-use solutions—civil-military applications—in the context of Poland, Europe, and NATO, which should consolidate the efforts of administration, business, and the military. The Prime Minister announced work on updating the blueprint for major cyber incidents as part of the Polish Presidency in the Council of the European Union in 2025.

Additionally, the Deputy Prime Minister presented the CyberTarcza (CyberShield) project, which aims to coordinate security reviews, build resilience, and respond to incidents. He announced a 3 billion PLN investment in CyberShield, with most funds going to local government institutions. The project includes developing local cybersecurity centres to support national-level CSIRTs, which will also receive additional support. He furthermore announced the establishment of the NASK Cybersecurity Center by 2029 and an increase in funding by 150 million PLN to support the recruitment of cybersecurity specialists in state administration. Mr Gawkowski emphasized the increased role of the Cybersecurity Coordinator, who will provide recommendations on cyberattacks to all industry entities and announced improvements in certification coordination and risk management. The Polish government will offer free training for both technical and non-technical personnel and ensure the development of digital skills. He also announced a new service in mObywatel – Bezpieczny w Sieci (Safe in the Web) – which will allow incident reporting, threat alerts, and provide a knowledge base on cybersecurity.

The Deputy Prime Minister concluded by emphasizing that cybersecurity is an inclusive area where all sectors and individual citizens must work hand in hand. He stressed that digital transformation is a key area essential for Poland's development.

ROAD TO THE POLISH PRESIDENCY 2025 – CYBERSECURITY PRIORITIES FOR EUROPE

The opening high-level panel discussion of the conference focused on the digital priorities for Poland's Presidency of the Council of the European Union in 2025. **Katarzyna Prusak-Górniak, Head of the Digital Affairs Unit in the Permanent Representation of Poland to the EU**, inaugurated the session by noting that from January 1, 2025, Polish diplomacy will oversee the work of several key Working Parties: Telecommunications and Information Society, The Horizontal Working Party on Cyber Issues, The Working Party on Data Protection, and the NIS Cooperation Group.

The first question was posed by the moderator to **Christiane Kirketerp de Viron, Head of Unit for Cybersecurity and Digital Privacy at DG CONNECT**. She inquired about the Commission's work during its current term. Ms Kirketerp de Viron provided a comprehensive summary of the EU Commission's intensive efforts over the past five years, highlighting initiatives such as NIS2, the Cyber Resilience Act, the Cyber Solidarity Act, the certification scheme, the establishment of the European Cybersecurity Competence Center, and dual-use initiatives. She also mentioned the 5G Toolbox, strategies for addressing the skills gap, and enhanced international cooperation.

PANEL DISCUSSION, 10:30-11:30
THE POLISH PRESIDENCY 2025
CURITY PRIORITIES FOR EUROPE
MAŁOPOLSK
MAIN PARTNER
Axel Deininger
Miguel Angel C ada
Host: Katarzyna Prusak-Gó

Deputy Prime Minister Gawkowski was then asked about Poland's plans for its six-month presidency. He articulated several priorities, including the elimination of cybersecurity silos, improved integration, and positioning Poland as a coordination agent between civilian and military sectors. He also emphasised the importance of supply chain security, open-source solutions, and crisis management frameworks. Furthermore, he underlined the necessity of updating the blueprint for the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, and the plans to enhance digital diplomacy.

Next, **Miquel Angel Cañada, Head of the National Coordination Centre (NCC-ES) at INCIBE**, shared insights from Spain's presidency and offered recommendations for Poland. Mr. Cañada highlighted three critical aspects of the Spanish presidency: reinforcing capabilities related to legislative initiatives of the European institutions, fostering dialogue with other regions on cybersecurity, and improving public-private cooperation.

Axel Deininger, Chairperson at ECSO, then provided the industry perspective on the future mandate of European institutions. He stressed the increased need for investments from both European stakeholders and nation states directed towards private stakeholders, considering a strategic 5–10-year outlook, particularly in response to the growing platformisation of cybersecurity. He also emphasised the necessity for robust yet manageable cybersecurity policies, citing the prolonged wait times and lack of coordination in the certification process of cybersecurity products, and the need to harmonise requirements.

Deputy Prime Minister Gawkowski concurred with the previous speakers, emphasizing the need to avoid creating additional regulatory requirements and administrative burdens for businesses. He advocated for greater clarity in implementing existing regulations, a sentiment echoed by Mr. Cañada and Ms. Kirketerp de Viron.

The second round of questions addressed the revision of the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. The speakers collectively agreed that the blueprint requires updating to reflect the current geopolitical climate, the need for simplified provisions, enhanced cooperation between military and civilian sectors, improved business continuity, and the integration of crisis management communities.

KI-ECSO LETTER OF INTENT SIGNING

The Kosciuszko Institute and the European Cyber Security Organisation have proposed a strategic cooperation aimed at bolstering European cybersecurity capabilities in anticipation of Poland's Presidency of the Council of the European Union in 2025. Together, they seek to elevate discussions on critical cybersecurity issues and drive positive regulatory changes within the EU framework, fostering innovation and resilience in digital technologies. The proposed collaboration includes a series of high-level events and workshops, spanning Brussels and Kraków, designed to gather policymakers, industry leaders, and experts. This partnership aims to generate actionable strategies and recommendations to fortify Europe's digital landscape, ensuring a secure environment for all stakeholders involved.

Prior to the official signing, the first speaker was **Deputy Prime Minister and Minister of Digital Affairs, Krzysztof Gawkowski**. He congratulated the Kościuszko Institute, a leader among non-governmental organizations in technology, on this initiative. He expressed hope that it would lead to better coordination between public administration, business, the military, academia, and the non-governmental sector. Next, **Luigi Rebuffi, Founder and Secretary General of ECSO**, mentioned the shared history of CYBERSEC and ECSO and demonstrated the intention and willingness to build cooperation among entities involved in this initiative to enhance not only Polish but also European cybersecurity. **Axel Deininger, Chairperson at ECSO** then stated that he also looks forward to cooperation and emphasized the important role of Poland in building the cybersecurity system and the involvement of Polish companies in the ECSO initiative. Finally, **Marietta Gieroń, Chairwoman of the Programme Committee of CYBERSEC** noted that signing the letter is an important milestone demonstrating shared commitment to enhancing cybersecurity capabilities through multistakeholder engagement. The format concluded with the official signing of the letter.

INTERNATIONAL SUPPORT FOR UKRAINE IN CYBERSPACE AND THE DIGITAL REALM – ROLE OF GOVERNMENTS AND THE PRIVATE SECTOR

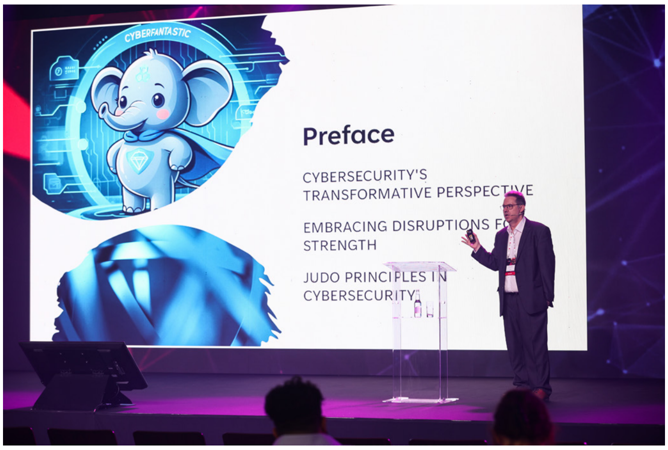
In the high-level fireside chat led by **Professor Paul Timmers, Research Associate, University of Oxford**, the focus was on the unfolding cyber dimensions of the Ukrainian conflict, resonating deeply with global efforts in cybersecurity and defense. **Tadeusz Chomicki, the Ambassador for Cyber & Tech Affairs at the Polish Ministry of Foreign Affairs**, highlighted the urgent need for coordinated international support, exemplified by initiatives like the Tallinn Mechanism. This mechanism aims to streamline aid efforts from NATO countries to meet Ukraine's evolving cybersecurity needs amid Russia's aggressive cyber tactics. Ambassador Chomicki pointed out successes such as providing crucial satellite communications and setting up mobile data centres to safeguard vital Ukrainian infrastructure.

Yuriy Gatupov, CTO and Co-founder of iIT Distribution, brought insights into how Ukraine's civil, private, and military sectors intersect in cybersecurity efforts. He underscored the pivotal role of companies, like Nova Poshta, in inadvertently supporting military logistics through their operational data. Mr Gatupov emphasised the ongoing need for cross-sector collaboration and preparedness, advocating for comprehensive cyber education from schools to professional training. Together, these perspectives shed light not just on the immediate challenges posed by cyber warfare, but also on the importance of sustained international cooperation and proactive resilience-building efforts across Europe.

The discussion illustrated the multifaceted responses required to navigate the complex cyber threats facing Ukraine and beyond. It underscored the critical need for innovative solutions, enhanced cooperation frameworks, like the Tallinn Mechanism, and a forward-thinking approach to cybersecurity that integrates civil, military, and private sector contributions. As Europe charts its strategic path in cyberspace, lessons learned from Ukraine are poised to shape broader conversations on digital sovereignty and resilience throughout the continent.

ANTYFRAGALITY – A PROACTIVE PARADIGM FOR THE FUTURE OF CYBERSECURITY

The keynote speech introduced "cyberfantastic," a proactive paradigm for the future of cybersecurity that emphasises embracing disruptive technologies. **Matthias Muhlert, CISO at Oetker-Group** explained that unlike cyber resilience, which aims to withstand threats, and antifragility, which evolves under adversity, cyberfantastic harnesses challenges to grow stronger. This approach moves beyond merely reinstating the status quo, making defence systems proactive and self-improving. Mr Muhlert outlined a five-stage progression for companies to achieve cyberfantastic: starting from ad-hoc security, moving through compliance-based modelling, a risk-based approach, proactive security,


CYBERFANTASTIC
Preface
CYBERSECURITY'S TRANSFORMATIVE PERSPECTIVE
EMBRACING DISRUPTIONS F… STRENGTH
JUDO PRINCIPLES IN CYBERSECURITY

and ultimately reaching cyberfantastic. Key concepts include self-regenerative systems, adaptive machine learning and AI, decentralised ID management, dynamic micro-segmentation, autonomous incident response, predictive analytics, quantum-resistant techniques, hybrid cloud resilience, and human-machine collaboration.

The speaker advocated for updating the traditional C.I.A. model (Confidentiality, Integrity, Availability) to the D.I.E. model (Distributed, Integrity, Exposure), which minimises single-point failures, ensures data integrity, and reduces data exposure. Mr Muhlert suggested using onion routing to implement zero trust principles in privacy protection, making IP addresses less identifiable. He emphasised the importance of introducing randomness in security and proposed that hacker principles could enhance data protection. Mr Muhlert concluded that risk management, though complex, is less critical in cyberfantastic, which should become the new defence and information security paradigm.

ELECTIONS UNDER THREAT – THE ROLE OF MEDIA IN COUNTERING DISINFORMATION

Ms Teresa Ribeiro, Representative on Freedom of the Media at OSCE, gave her perspective on current processes in the information sphere. She underlined that free and independent media are essential in every democratic society. We need trustful information with multiple perspectives to have a healthy public debate with informed citizens. Cyberattacks paired with disinformation can amplify small events to polarise the voters, and with the increasing use of AI in election campaigns, the challenges will only become bigger. Cyberattacks and disinformation might try to undermine the democratic process by interfering with the integrity of the electoral process through media regulation. Media freedom is essential because it connects human rights, democracy and security. It needs legal protection, technological, financial, and human resources to ensure that the public continues to be well informed. Ms Ribeiro underlined that we need a new concept which is a public interest framework that endures media freedom and availability of quality information, enabling debate and scrutiny of those in power. We need technology to boost democracy. Ms Ribeiro concluded that problems of disinformation and cybersecurity cannot be solved by blocking and banning, but with the availability of quality information.

SAFEGUARDING THE PROGRESS. EUROPEAN CYBERSECURITY INDUSTRY HALFWAY THROUGH THE DIGITAL DECADE

In her post-lunch keynote address, **Christiane Kirketerp de Viron, Head of Unit for Cybersecurity and Digital Privacy at DG CONNECT**, presented the current state of the European cybersecurity industry. Ms Kirketerp de Viron emphasised that having a robust cybersecurity industrial ecosystem is crucial for European resilience. She began by comparing figures, noting that the European cybersecurity market, excluding the UK, accounts for 17% of global value. Out of the world's 500 largest firms, only 67 are based in Europe. Examining mergers and acquisitions in the cybersecurity market, in 2023, 41 of 180 companies were acquired by non-EU players. Additionally, non-EU entities control a significant portion of the European market – up to 75% in the civilian sphere and up to 20% in the defence-military sector.

She also highlighted the fragmentation of the European market, with 97% of companies being SMEs, while large companies still take home 97% of all revenue generated. Ms Kirketerp de Viron stressed that cybersecurity is a growing market, largely due to geopolitical factors, but the lack of skills is hampering this growth. She noted that the European Commission is also contributing to market growth by citing regulations within NIS2 and the Cyber Resilience Act, which are raising cybersecurity requirements and thus creating business opportunities. The key question, according to Ms Kirketerp de Viron, is how we are going to ride this growth.

The first requirement is to address the skills gap, which currently amounts to 357,000 people needed in cybersecurity. This gap must be filled not only by cybersecurity professionals but also by those working in AI, quantum, software engineering, and finance who understand cybersecurity. In terms of investments, there is room for improvement. In 2023, funds raised in the cybersecurity sector decreased by 42%, and there is currently an investment gap of 1.75 billion euros in Europe, along with a significant shortfall in venture capital investments compared to other global players.

Going forward, we need to focus on skills development, creating conditions for ecosystem growth by collaborating with venture capital, equities, and leveraging public-private partnerships in this field. It is also important to adopt a streamlined approach to investments in dual-use technologies. Additionally, more attention must be paid to emerging technologies such as AI, quantum computing, cryptography, and especially post-quantum cryptography.

Given these challenges, Ms Kirketerp de Viron underscored the importance of initiatives like establishing the European Cybersecurity Competence Center, eliminating fragmentation, and developing synergies between civilian and military sectors.

DUAL-USE TECHNOLOGIES – CIVIL-DEFENCE COOPERATION IN CYBERSPACE

The evolution of cybersecurity discourse has shifted from a stark division between military and civilian realms to a critical focus on collaboration, as highlighted by **Jean-Marc Wasilewski, Retired Major General at Signal Corps of the French Army**. He noted the differing organisational structures, decision-making speeds, and resource allocations between private and military sectors, underscoring the need for enhanced trust and information sharing. Wasilewski emphasised that defence sectors must share intelligence with civilians to bolster overall security. **Col. Jarosław Wacko, Lead Specialist at Polish Cyber Command**, pointed to Ukraine's successful model of intersectoral cooperation, protecting critical infrastructure like energy, healthcare, and financial systems. Wacko also raised concerns about frequent attacks by state-sponsored groups from Eastern Europe targeting Poland and other Ukraine supporters, stressing the importance of assisting contractors in securing their networks, systems, and shared information. Despite historical trust issues, Wacko noted that cooperation is improving, although challenges remain.

Tomasz Husak, Adviser for Digital Agenda and Data Technologies at DG INTPA exemplified the evolving cooperation between civilian and military spheres in the space sector, with EU space policy increasingly incorporating military standards. He cited the Galileo constellation, originally for civilian use, now including the military-specific Public Regulated Service. Husak also mentioned that Earth observation constellations are being adapted for governmental applications, and the Iris Square constellation for communication aims to provide robust, low-latency communication for government and military use. **Jonas Cederlöf, Policy Officer at DG DEFIS, European Commission**, stressed that while cyber defence efforts aim to harness synergies, the distinction between civil and military domains remains clear. **David Antunes, Cyber Defence Programme Manager, European Defence Agency** highlighted that public-private partnerships are indispensable for integrating civilian-driven cyber expertise into defense strategies. Mr Antunes also discussed the importance of dual-use capabilities covering peacetime, crisis, and total war, extending to exploitation, intelligence, and power projection. Technologies like augmented reality, virtual reality, cloud, edge, and fog computing are vital for dual-use in education,

training, and enhancing cyber situational awareness. Mr Husak concluded by emphasising the European Commission's recommendation for secure and resilient submarine cabling, highlighting the need for defence engagement and greater oversight of cable ownership and operations to improve security and resilience.

ENTERING AN ERA OF CYBER REGULATION IMPLEMENTATION

The next panel started with introduction from its host, **Andrzej Bartosiewicz - President of the CISO #Poland Foundation and founder of CISO4U**. During a dynamic panel discussion on European cybersecurity regulations, speakers highlighted the critical need for strategic cooperation between the private sector and governments to enhance Europe's competitive edge. **Rita Jonušaitė, Senior Manager for Cybersecurity & Cloud at DIGITALEUROPE** emphasised that the focus should now be on the effective implementation of existing regulations, which she believes will spur competitiveness if done correctly. She also stressed the importance of innovation in defence mechanisms to match the constantly evolving attack methods, suggesting that guidelines and templates, particularly for smaller companies, could streamline the regulatory process and reduce unnecessary reporting burdens.

Mateusz Stefański of Alior Bank and **Florian Pennings from Microsoft** pointed out that directives like DORA and NIS2, while foundational, require nuanced implementation at the national level to be effective. Mr Pennings illustrated the differing cybersecurity perspectives between Brussels and national capitals, and **Zuzanna Wieczorek, CEO of Tekniska** noted the low maturity levels in many industries regarding security compliance. The conversation underscored the importance of integrating various regulations, such as the Cyber Resilience Act and AI Act, into a cohesive strategy. The panelists collectively highlighted the need for clear, standardised regulations to facilitate smoother compliance for SMEs, with a call to reduce administrative burdens and promote robust cybersecurity measures across Europe.

TRACKING ADVERSARY: TRENDS AND DEVELOPMENTS IN THE CYBER THREAT LANDSCAPE

The aim of the presentation from **Crowdstrike's Gabriel Kujawski** was to showcase that there is no malware problem; instead, there is an adversary problem, with 75% of attacks last year not involving typical malware. Attackers are using tools undetectable by traditional methods, making it crucial to track their tactics and identify their modus operandi. Human-operated attacks are increasing, with a huge percentage of cases involving direct interaction, and attackers are moving laterally within organizations faster, reducing the time from 84 to 62 minutes on average in the last years. Criminal groups and APTs are shifting away from malware, exploiting human vulnerabilities, and focusing on identity-related attacks. They have also improved their skills in targeting public cloud infrastructures and supply chains. Additionally, AI tools like ChatGPT are being used for sophisticated phishing and information attacks, with young cybercriminals increasingly using AI to enhance their operations.

ECCC VS DIGITAL EXPERTISE SHORTAGE

Luca Tagliaretti, Executive Director of the ECCC, emphasised the crucial mission of the ECCC to bolster Europe's resilience against cyberattacks, enhance the competitiveness of European companies, and re-

juvenate investment in research. He highlighted that addressing cyber skills is currently one of the most challenging issues due to several factors: the need for 200,000 to 500,000 professionals to ensure cybersecurity resilience, the complexity of coordinating efforts to close the skills gap, the ever-evolving nature of this gap, and the time required to revamp education and career pathways. Mr Tagliaretti stressed the importance of focusing on both the human and technological aspects of cybersecurity. The ECCC is fostering partnerships between industry and academia to establish a unified European skill framework and has invested significantly in a user-friendly online training platform to mitigate and respond to threats. Looking ahead, Mr Tagliaretti mentioned the aim to involve the national coordination centre more extensively to harmonise responses at the local level, projecting that by 2027, the impact of these policies and efforts should be evident in narrowing the skills gap.

MIND THE SKILLS GAP

After the introduction by **Luca Tagliaretti, Executive Director of the ECCC**, the host **El Iza Mohamedou, the Head of the OECD Centre for Skills** started the panel by highlighting that a vast amount of money, around $3.5 billion, is at threat due to cybersecurity challenges and that we need to focus on the shortage of a skilled workforce in order to solve this issue. When asked what role governments can play in creating a more skilled workforce, **Michał Pukaluk, Deputy Director of the Cybersecurity Department at the Ministry of Digital Affairs of Poland**, said that “every government has to experiment – look around if there are any lessons learned or good practises that can be applied.” He continued to talk about the ministry’s program PWCyber, which utilizes public and private partnerships for cybersecurity training. Partnerships and programmes became popular topics amongst the speakers as they all introduced their platforms which bring cybersecurity training and education closer to professionals and the general public.

As highlighted by **Luigi Rebuffi, Founder and Secretary General of the European Cyber Security Organisation (ECSO)**, the problem lies not only in the competency of the workforce, but also the competency of society as a whole. This is why ECSO has the Road to Cyber platform, which is aimed at the youth, and provides the participants with the proper skills and knowledge to join the workforce. This also creates lifelong education as cybersecurity is a constantly evolving field and constant education is key to understanding it.

Following the theme of education, **Yann Bonnet, Deputy CEO of Campus Cyber** reflected on the evolution of trainings offered to the youth in France. Training and education innovation evolved to make the courses more attractive and started an initiative to show diversity in cybersecurity jobs as a response to the high number of girls dropping out from science related fields early on in life.

A critical part of the conversation came about when Mr Tagliaretti brought attention to the fact that we have to really “map” the skills gap rather than mind it, because it allows us to understand the root of the issue and therefore helps us find effective ways of solving it. **Maria Caruso, Government Affairs Specialist at the European Government Affairs in Microsoft**, stated that “the Microsoft Digital Defense Report highlighted that in 2023 alone, there has been a 35% increase in the demand for cybersecurity skills.” This sparked the debate on the most effective method of mapping the skills gap, such as partnering with local governments, businesses, educational institutions and non-profit organisations.

As stated by Mr Tagliaretti, “collaboration is at the core of our mission.” All speakers spoke about their collaboration with multiple stakeholders in order to map the problem and create programmes targeted at local needs. Continuous education, partnerships, and a clear united vision are the foundations for decreasing the skills gap and were highlighted by all speakers involved.

UNCOVERING GENDER-BASED DISINFORMATION IN POLISH POLITICS

Men = political critiques
Women = critiques based on characteristics
Insulting a woman's intelligence = Women less intelligent
Women are too emotional for politics = Women emotional
Any feminist or woman who doesn't embrace is a threat to soci
A woman's main role is being a mother
Critiquing women based on their physical ap = Women expecte
look good attention to their

The programme of the day concluded with a presentation by **Eliza Kotowska, Analyst and Project Coordinator at the Kościuszko Institute**. Ms Kotowska started the presentation by defining gender-based disinformation as the spread of false information intended to harm or discredit a person based on their gender. She highlighted that it is most frequently used against women in politics, seeks to discredit them based on their gender and is often accompanied by hate speech, which like gendered disinformation, utilises gender stereotypes. She presented some of the most common hate speech and disinformation narratives in the polish cyberspace which focused on women being mothers, too emotional, less intelligent and too sexual for the workplace. Using these narratives, accounts on social media such as X, Facebook and Instagram, used these narratives to portray the message that a woman is not fit for politics. “Female candidates have a harder fight because their gender is enough to discredit them. Not only do they have to fight disinformation which exists about the topics for which they stand and prove that their ideas will be beneficial, but they first have to prove themselves worthy of even being in the spotlight.”- Eliza Kotowska.

FORUM STAGE, 20 JUNE

CYBERSECURITY INVESTMENTS IN CEE

The second day of the conference started with a panel discussion hosted by **Joanna Świątkowska, Deputy Secretary-General of ECSO** who initiated the discussion by highlighting that Europe is still behind countries like the US when it comes to investments into cybersecurity markets. **Aleksander Mokrzycki, Member of the Board of PFR Ventures**, highlighted that the CEE region is further behind the EU partly due to the insufficient amount of investment from both the government and private sector.

Carlos Moreira da Silva, Founder and Managing Partner of 33N Ventures explained some of the root causes of the lack of investment, such as the lack of capital and specialised support to help companies become leaders. Mr Moreira da Silva expanded on Mr Mokrzycki's words by stating that "the European cybersecurity spending market is roughly 30% of the global market, which makes it a very interesting market for every player that wants to be a global leader, but still our quota of the global investment is 10-20%." He explained that in order to address this dilemma, we must support companies to scale up and become global leaders and avoid the large brain drain and investment movement to other countries.

Patric Gresko, the Head of Division for Innovation and Sustainability at the European Investment Fund spoke about funding whole ecosystems by "making sure that they [CEE cybersecurity companies] have the basic key ingredients to raise a second, a third fund, and eventually seven generations of funds to become autonomous and independent from any public funding." Mr Gresko also brought up the topic of private and private partnerships. Funding from EU agencies in collaboration with member states attracts corporate investors interested in that specific ecosystem.

Upon answering the questions of how the war on Ukraine has affected these investments and the role of individual investors, the speakers spoke of involving more investments from the private sector, mobilising other sources of capital, and the European cybersecurity market becoming more independent. The conclusion of the panel highlighted the importance of a more united and sovereign European cybersecurity market.

WIRED FOR SUCCESS? EMPOWERING EUROPE'S DIGITAL INFRASTRUCTURE

The agenda continued with another panel discussion focusing on Europe's digital infrastructure. The panel's host, **Tomasz Piekarz, a Senior Specialist at the Ministry of Diigital Affairs of Poland**, explained how the Digital Networks Act, introduced last year, aims at fostering European telecom champions, bridging investment gaps, fostering innovation, ensuring security, and leveraging the Single Market to advance digital sovereignty. However, concerns have surfaced regarding the necessity to strike a delicate balance between incentivising investments and ensuring fair competition, potential adverse effects of deregulation, and alignment with sustainability objectives.

According to **Dr Joanna Kulesza, Assistant Professor of International Law at the University of Lodz and the Director of Lodz Cyber Hub**, unlike U.S. business methods, when it comes to legislation, Europe prioritises the protection of the individual over the company. While the people feel more protected, the downside of this is that it creates a tougher environment for innovation for young companies. This came as a response to whether Europe is losing its technological competitivity.

Lise Fuhr, Director General of the European Telecommunications Network Operators' Association spoke about how European competitiveness is the key strategic aim for the future and simultaneously an economic challenge. Ms Fuhr highlighted the role of digital infrastructure in this competitiveness, and underlined that Europe is losing in the innovative part.

Marc Vancoppenolle, VP of Government Affairs EU & Europe at NOKIA, spoke about the role of 5G in unlocking European potential. Mr Vancoppenolle mentioned how 5G can help with industrial internet which in turn plays a role in advanced digitalisation that can strengthen sectors, such as energy and defence. **Ingrida Taurina, the Head of the Executive Director's Office at ENISA**, continued to speak about European potential by referring to the White Paper which helps Europe by providing a general view of future challenges and recommendations for the member states. Ms Taurina continued to mention the NIS cooperation group which further strengthens Europe's potential by meeting together to discuss the gaps and recommendations in cybersecurity.

The discussion turned to the security of outer space and the standardisation of cybersecurity. Dr Kulesza pointed out that while the EU may have lost its battle in 5G against powers like China, we still have a chance for creating a stable infrastructure for lower orbit satellites. Mr Vancoppenolle and Ms Taurina continued the discussion on standardisation by claiming that standardisation has to be unified globally and discussed together with companies.

When talking about other topics, such as quantum, all speakers referred to a similar harmonised approach. This summarises the discussion very well, as most of the speakers referred to partnerships, cooperation and a unified strategy in order to empower Europe's digital infrastructure.

SECRET? MIDNIGHT? BLIZZARD? OR PERHAPS SIMPLY AN INCIDENT THAT'S WORSE THAN IT MAY SEEM?

In January 2024, Microsoft announced that Russian services had gained access to its infrastructure. Simultaneously, someone obtained administrator privileges in Office 365 within a small Polish non-governmental organisation. Were these two incidents related? How did malware files appear on workstations undetected by antivirus programs? During his exclusive on-site presentation, **Maciej Broniarz, Chief Executive Officer at DeCode9 and Executive Board Member at RIFFSEC**, showcased how such incidents unfolded, how criminals infected victims' computers, escalated privileges, gained persistence, and managed to hide in victims' infrastructure for several months.

BUILDING EUROPEAN CYBERSECURITY UNICORNS – UTOPIA OR AN INEVITABLE FUTURE?

The agenda continued with another panel discussion that was moderated by **Karol Tokarczyk, a Senior Analyst for Digital Economy at Polityka Insight**, who started by focusing on the definition of cybersecurity unicorns. **Karel Obluk, Partner at Evolution Equity Partners**, began by stating that most tech unicorns can be found in North America rather than Europe. **Patrick Gresko, Head of Division for Innovation and Sustain-**

ability at European Investment Fund, agreed with this point and the fact that in Europe, the term unicorn still applies, as there are many more cybersecurity unicorns in the United States. There is a huge gap in the amount of start-ups in the US versus Europe. Both speakers addressed the issue of European unicorns starting in Europe and moving their operations to the United States, which weakens Europe's potential.

Maria Magdoń, Head of Division at the Department of Digital Economy at the Ministry of Economic Development and Technology, added the Polish perspective that unicorns are vital because they are part of Europe's digital decade. **Eryk Libelt, an expert in new technologies, investor and member of the Advisory Board of Polish Cluster #CyberMadeInPoland**, concluded the first round by saying that he predicts that there will be a spike in the number of unicorns in the near future.

The discussion continued to cover the influence of the Russian-Ukrainian War on investments such as an increase in interest in cybersecurity start-ups, higher revenues, increased interest from investors, and higher demand for products and solutions. The conversation then moved to the Polish approach to delivering the solutions needed by these unicorns, which often deal with a lack of competence, financial barriers, and the lack of a long-term strategy. Continuing the theme of supporting cybersecurity start-ups, Mr Obluk and Mr Gresko spoke of a closer cooperation between large enterprises and start-ups from their regions.

When talking about challenges that unicorn ecosystems face, the speakers spoke of finding good companies and ideas, difficulties finding talent from abroad, poor business models, keeping companies in Europe, and building the skills of the future generations. When asked about concrete steps that are being taken to address these issues, the speakers focused on partnerships with academia as well as thegovernment. For recommendations, many of the speakers suggested that start-ups focus on their local market before reaching out to other regions.

STRENGTHENING NATO'S CYBERSECURITY POSTURE

The first round of questioning revolved around artificial intelligence and cyber defence and their use by APT groups. **Nikolas Ott, Senior Manager of European Government Affairs at Microsoft**, stated that three pillars are essential in differentiating and finding similarities between AI evolution and traditional cyber security, including: cybersecurity for AI, AI for cybersecurity, and AI-enabled cyberattacks. Red teaming defence procedures were labelled as an extremely important process because AI models cannot be updated easily. AI is able to give defenders advantages by detecting attacks more quickly. However, APT actors are using AI models to generate phishing attacks. The tech accord has been created, which outlines concerns regarding AI and disinformation, particularly with deepfakes. The speaker then asked if AI was being used or just being observed to be used by opponents and whether the use of AI was more in the private sector or military sector. **Col. Jarosław Wacko, Lead Specialist in the Polish Cyber Command**, then answered that the military is already using AI for detection and correlation of discrepancies in data. **Jacek Niedziałkowski, Security Solutions Senior Sales Manager at IBM**, then advocated for a military approach to civilian and private sector cyber security, as practices and structures used by the private sector work very well within a time of peace, but that because of Russia's war in Ukraine that Europe and NATO are in a time of war necessitating greater awareness and readiness. **Commander Davide Giovannelli, Leading Researcher at the Law branch of NATO CCDCOE**, stated that the Tallinn manual is confusing and often contradictory, and that a new toolkit is being developed to give more concrete answers to legal questions in the context of Russia's war in Ukraine. Another challenge is classifying, reacting to, and carrying out below-attack

cyber operations. Furthermore, it is legally unclear whether a countermeasure to a cyber operation could be applied in a collective manner through the alliance. Col. Wacko stated that collective defense is being trained through team-based competitions that include joint teams, and the differences between the teams are becoming smaller because cybersecurity throughout NATO countries continues to grow through the exchange of best practises and cooperation.

The host, **Mirosław Maj, Founder and President of the Safe Cyberspace Foundation**, then asked Mr Niedziałkowski and Mr Ott about the challenges of responding to below-threshold cyber operations as members of the private sector. Mr Niedziałkowski responded that the private sector can make recommendations for future preparation. Mr Ott recommended that certain best practises should be adopted: legally, the Oxford Process should be promoted to solve complex grey zone ambiguity. Furthermore, industry leaders, such as Microsoft, should be involved in NATO training exercises, however clear boundaries should exist regarding the different responsibilities of governments and private companies in the context of hybrid warfare. In closing, the speakers were asked how they would strengthen NATO's cybersecurity. Mr Ott emphasised that governments should strive to see dual-use potential in commercial tools, and they should do so at the correct pace. Mr Niedziałkowski argued to raise awareness of cyber security threats, and the host concurred and stated that a mechanism is needed to be created for this. Col. Wacko argued that DCO and OCO are well prepared, but that trust between the military and society needed to be enhanced and that active defence needed to be increased. Commander Giovannelli noted that cyber defence is expensive and evolving, and that funds for the future need to be secured.

UNDERSTANDING AND HACKING AI IN 2024

The speaker, Mateusz Chrobok, cybersecurity, AI and startup consultant, stated that AI is everywhere; it has been implemented in a myriad of sectors and also influences human decision-making. He argued that data bias has a significant impact on AI models, as many AI models are racist or bigoted due to corresponding data found on the internet. The most popular method for the creation of an AI model is HRLF, or Human Resource Learning Feedback, in which a human is given a question and an answer which the model learns from. However, the model also learns human bias and responds to the culture in which it is built. Big Language data, when an AI model is kept away from the outside world during its training, is an improvement from this bias because the context of its development is more controlled. Large companies have pooled their data resources to train AI models. However, data collection is a nebulous term, and it is unclear how much data is being farmed. AI models that are trained on open-source data can disseminate disinformation and violate copyright laws. A solution to the copyright problem is to 'poison the well' or use adversarial imagery to trick AI models into providing incorrect responses to stimuli. This has caused AI models to incorrectly answer basic questions, as has incorrect or satirical data from Reddit. Only 0.01% of data or examples need to be adversarial to poison an LLM. This is impactful because election information and individuals' decision making can be targeted by poisoning influential AI systems. It is easy to influence worldviews when advertisement profiling is understood. ChatGPT can also accidentally reveal secrets or hallucinate if given adversarial examples, but implementing opening and closing mechanisms can make AI models more efficient at doing math. Furthermore, models have evolved to not give answers that could cause harm to the population, but these limitations can be broken in several ways.

CLOSING

The speaker, Grzegorz Żych, Director of the Centre for Information Technology Services of the city of Krakow, began the closing by giving a brief summary of some of the main points highlighted at the conference thus far, including investments, completing the confidence gap, and cybersecurity of outerspace. Furthermore, he supported the business and networking aspect of the conference and raised the importance of building awareness of cybersecurity and expressed joy that politicians are taking a stand in this realm.

NCC-PL

DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI
DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI

EXPO STAGE, 19 JUNE

SOC NETWORKS – EUROPE'S CYBERSECURITY SHIELD

The panel discussion emphasized the critical need for the introduction of SOC networks due to unprecedented cybersecurity demands. The host, **Ewelina Kasprzyk, R&D&I Specialist at the AGH Cybersecurity Centre**, began the panel by highlighting the vulnerabilities of the academic sector in the context of malware attacks. Ms Kasprzyk continued to briefly elaborate on the SOCCER program, which is a collaboration of universities who are working together to improve SOC competencies in the CEE region.

The first question, directed at **Col Jarosław Wacko, Lead Specialist at the Polish Cyber Command**, aimed to establish the current threat which the Eastern flank of NATO is facing. Col Wacko explained that the biggest threat affects both the military and civilian sectors, relates to the current Russian-Ukrainian War, and is at a level which has not yet been previously seen.

Krzysztof Sierański, Member of the Board at STILLSEC, spoke about the lack of understanding amongst the clientelle about their own cybersecurity needs and how SOC networks can help them. **Tomasz Gładkowski, COO of 4Prime Sp. z o.o.** concurred with Mr Sierański about the amount of clientele who are not educated enough about SOC networks and therefore do not know how they can help them. He then continues to highlight the importance of creating a system which allows firms to detect threats, as to better their understanding of their own needs. Col Wacko added to this topic by saying that competencies of workers have to go hand in hand with platforms and programs than help firms detect threats.

This sparked a conversation about the necessary teamwork between SOC network specialists and the companies and the benefits of creating a collaborative network of threat detection. As stated by Mr Sierański, SOC networks are only one tool for cybersecurity and businesses should be utilizing it along with other cybersecurity measures. The theme of cooperation and partnership continued when Col Wacko spoke about international partnerships and the importance of secure and trusted information exchange. Mr Gładowski concurred with Col Wacko by elaborating that trust is a necessary aspect so that quality information can be exchanged for closer analyses and inspections of threats.

In summary, the speakers underscored the necessity of enhancing visibility and awareness of these networks. They highlighted the importance of educating clients on their specific needs and the role that SOC networks play in addressing them. Finally, they also focused on the imperative of collaboration with IT specialists and secure information exchange as key components of future cybersecurity strategies.

CAN GENERATIVE AI OPRIMISE OFFENSIVE SECURITY?

Michał Suchocki, Co-creator and Chief Product Officer at CyCommSec, discussed the creation of thinking agents in AI tools, such as Chat GPT. He explained how these agents can enhance the quality of basic commands through reflection, tool use, planning, and multiagent collaboration. Suchocki emphasised that these advanced AI approaches can be effectively utilised to detect online vulnerabilities, thereby significantly enhancing our resilience against cyber threats.

MONITORING EMPLOYEES AND EXTERNAL CONTRACTORS – 5 BEST PRACTISES

Paweł Chudziński, CEO of Securivy, Ekran System Polska, presented on the best practises for monitoring employees, external contractors, and privileged users. He demonstrated how utilising jumpserver architecture can be beneficial to both the company and its employees, provided that a proper dialogue is maintained.

CYBERSECURITY OF OPERATIONAL TECHNOLOGY AS A FOUNDATION OF THE NEXT GENERATION INDUSTRIES

Andrzej Cieślak, Founder and CEO of Dynacon, emphasised that cybersecurity is the cornerstone of next-generation industry. His presentation showcased the importance of integrating physical systems, the physical environment, monitoring, and technology in bolstering cybersecurity. The systems highlighted during the presentation illustrated various methods to help businesses enhance their cyber resilience.

BEST PRACTICES FOR THE IT DEPARTMENT FROM THE NIS2 PERSPECTIVE

Piotr Adamczyk, Technical Account Manager at Axence, discussed the requirements of the NIS2 directive, which mandates that essential and important entities conduct risk analysis, manage incidents, and implement cybersecurity education programs for employees. He focused on how Axence's ITAM system assists businesses in managing incidents, conducting risk analysis, and effectively educating employees about social engineering and phishing threats.

BUILDING AND MAINTAINING SOC IN YOUR ORGANISATION – THREE CHALLENGES

Michał Horubała, Director of the Security Operations Center at SOC360, 4Prime IT Security, discussed building and maintaining a 30-person SOC team that protects Poland's largest commercial organisations. He highlighted challenges such as the shortage of qualified cybersecurity specialists, insufficient educational preparation, 24/7 scheduling, and adapting remunera-

tion systems. Horubała emphasised the need for flexibility in addressing dynamic cyber threats, as rigid playbooks are inadequate, requiring continuous measurement and analysis by SOC analysts.

SECURING CRITICAL TELECOM INFRASTRUCTURES – INCREASED VALUE AT RISK IN 5G

German Peinado Gomez, Principal Standardisation Lead at NOKIA, discussed securing critical telecom infrastructures during the transition to 5G networks. Emphasising the importance of interoperable security standards and protocols, he highlighted challenges in adhering to standards like GSMa and the EU's Cybersecurity Act. The session stressed the need for robust security measures against evolving cyber threats, advocating for multi-layered defense strategies and specialised tools tailored for telecom protocols.

IN SEARCH OF TRUSTED AI: THREATS AND SOLUTIONS IN ACCORDANCE WITH ISO/IE 42001

Tomasz Szczygieł, Information Security Officer, Data Protection Expert, and Auditor, in his presentation emphasised the identification of key threats linked to artificial intelligence (AI) and proposed solutions aligned with the ISO/IEC 42001 standard. The presentation highlighted AI's expanding integration across sectors such as healthcare and finance, stressing the critical importance of trust for its safe and accepted deployment. Challenges discussed included algorithm transparency, biased data, and security vulnerabilities, underscoring the need for meticulous adherence to standards like ISO 42001 from the outset.

WHY YOUR BUSINESS CONTINUITY PLAN DOESN'T WORK: TOP X MISTAKES EVERY CISO MAKES

Gregory Zagraba, Presales Engineer at Xopero Software & GitProtect.io, discussed the evolving and unpredictable cybersecurity landscape. He emphasised that outdated security policies, recycled from past templates, are inadequate in today's dynamic environment. Zagraba highlighted the importance of a comprehensive Business Continuity Plan (BCP) to ensure organisational stability during crises, stressing that it should encompass guidelines anticipating all potential scenarios. The presentation also identified common mistakes

GitProtect
by Xopero ONE
Why Your Business Continuity Plan Doesn't Work?
Top X Mistakes Every CISO Makes

made by CISOs, including selective risk analysis, neglecting data classification for backups, overlooking factors affecting backup speed, lack of automation in backup processes, inadequate data protection, narrow disaster recovery plans, lack of scalability in backup and disaster recovery solutions, and over-reliance on cloud vendors.

PRESENTATION UNDER THE PATRONAGE OF THE MALOPOLSKA REGION: POLAND ON THE DIGITAL FRONT LINE

The presentation, under the patronage of the Malopolska Region, began with a speech by **Deputy Marshal of the Malopolska Region, Józef Gawron**. This was followed by **Dominik Rozdziałowski, Director of the Department of Cyber Security, Ministry of Defense**. During the presentation, three main operational sectors of the Polish Cyber Defense Forces were discussed: IT, cyber, and crypto. IT involves designing networks and IT solutions, crypto deals with cryptographic security, and cyber constitutes a crucial element of defence, encompassing both active and offensive operations. Last year, CSIRT MON recorded 5,841 incident reports, most of which were related to phishing campaigns often linked to the situation in Ukraine. These attacks were carried out by Russian groups APT-28, APT-29, and Turla, each with different techniques and objectives.

Dominik Rozdziałowski emphasised the growing need for the development of drone and satellite technologies to better monitor the battlefield and make rapid decisions. Attention was drawn to the necessity of introducing forensics at a lower military level and modernising command posts. A key element of future operations will be artificial intelligence, whose application in analysing data from drones and satellites can significantly enhance operational efficiency. The Polish military is actively learning from both Ukrainians and Russians to strengthen their skills.

NETWORK SUPER DETECTIVE

In his presentation, **Karol Kij, Director of Cybersecurity Solutions at Atende**, introduced Network Detection and Response (NDR) technology as a crucial element of a modern security strategy. The presentation explored how NDR functioned as a vigilant super detective, constantly monitoring network traffic, identifying anomalies, and promptly responding to potential threats in real-time. By presenting the power of behavioural analysis techniques, artificial intelligence, and real-world case studies, the aim was to exhibit a sense

of security and confidence in participants. They gained insights on effectively integrating NDR with their existing security systems, thereby enhancing the protection of their IT infrastructure.

Cyber Attack - any kind of malicious activity that
attempts to collect, disrupt, deny, degrade, or destroy
information system resources or the information itself
Attack = BIG PROBLEMS
WE HAVE A

ROLE OF THE SECURITY OPERATIONS CENTRE IN BUILDING CYBER RESILIENCE OF THE ORGANISATION

The Security Operations Centre (SOC) has risen to prominence in recent months as a critical service in addressing escalating cyber threats. **Grzegorz Gąsiewski, Systems/Business Analyst at Perceptus**, discussed the pivotal role of SOC in solving cybersecurity challenges. He highlighted how SOC provides real-time monitoring and response capabilities round-the-clock, ensuring immediate detection and mitigation of threats. The presentation delved into specific capabilities and practical applications of 24/7 monitoring, emphasising tangible outcomes beyond theoretical promises in enhancing organisational cybersecurity posture.

CRITICAL CONNECTIVITY AND VIDEO CONFERENCING SECURITY IN COMPLIANCE WITH NIS2

Changes in regulations concerning IT systems, their security, and operational continuity were affecting numerous entities across Europe. In the era of video presence and hybrid meetings, a video conferencing system in every organisation had become a critical tool for operational functionality. During the presentation, **Zygmunt Łodziński, Vice President of Operations and COO at Visioncube**, addressed aspects related to the security of audio and video communications, securing content at the media level, and raised doubts about using popular cloud platforms for conducting critical meetings. These topics were rarely discussed openly, and the insights shared during the presentation enlightened participants and redefined their perspectives on the security of communication systems.

ARTIFICIAL INTELLIGENCE IN THE SERVICE OF (IN) SECURITY

Artificial intelligence has become increasingly prevalent in our lives, impacting various aspects of security. The presentation addressed how AI can be easily mis-

# Konwersja hasła na SecureString
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
# Generowanie klucza na podstawie hasła
$key = (New-Object System.Security.Cryptography.Rfc2898DeriveBytes
Get-ChildItem $folderPath -File | ForEach-Object {
$content = Get-Content $_.FullName -Encoding Byte

used and highlighted the risks associated with its application in security. **Daniel Wysocki, Head of the Cybersecurity Department at Advatech**, elucidated these points to enhance participants' awareness of both the benefits and potential pitfalls of utilising AI for security purposes.

FUNDING EUROPEAN CYBERSECURITY ECOSYSTEM

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Funding European Cybersecurity Ecosystem
Alina TARALUNGA, Programme Officer
Michal REKOWSKI, Programme Officer
19.06.2024 - Krakow

Michał Rekowski, Programme Officer at the ECCC, gave an overview of the foundation of the ECCC, which occurred concurrently with the formation of the network of NCCs and the Competence Community. The ECCC is the engine for the implementation of Europe's cybersecurity policies, most importantly managing development funds and raising awareness of funding and cybersecurity development. Every EU nation creates an NCC, which is managed by the ECCC along with the Competence Community. The ECCC responds to challenges and connects the European cybersecurity base in order to raise awareness and increase competitiveness within a mature global market. The ECCC's bodies that manage funds are Digital Europe (DEP) and Horizon Europe. There are three implementation tools within the EU's current cybersecurity strategy: regulation, investment, and policy initiatives. These tools are complemented by the pillars of resilience, technological sovereignty, and leadership; building operational capacity to prevent, deter, and respond; and cooperation to advance a global and open cyberspace. **Alina Taralunga, Programme Officer at the ECCC**, then outlined the portfolios and funding opportunities provided by the ECCC. The DEP's project portfolio includes the Cyber Alert System, Cybersecurity in Health, Novel Applications of AI, Transition to Post-Quantum Cryptography, 5G Infrastructure, and Support to EU Cyber Legislation. The beneficiaries of this program include a myriad of sectors, and there is a call for open submissions for grants on July 4th, 2024. The Horizon Europe program is slightly different, and rests upon the pillars of scientific excellence, global challenges and competitiveness, and innovation for project funding. The project portfolio of this fund includes infrastructure resilience, security quantification, hardware, software, and supply-chain security, advanced cryptography, AI and cybersecurity, and security, privacy, and ethics.

EUROPEAN DEFENCE FUND 2024 – CYBER OPPORTUNITIES

The European Defence Fund is about maximizing the outcome of defence spending by focusing on research and development. The presentation explained the role of the member states in drafting projects and topics and where cyber focused activity falls within the defence centred projects.

In his presentation, **Jonas Cederlof, Policy Officer at DG DEGIS, European Commission**, delved into the workings and goals of the European Defense Fund (EDF), a program aimed at bolstering defense capabilities through research and development. The EDF is fundamentally about maximizing the effectiveness of defense spending by focusing exclusively on research and development. This initiative encourages cross-border collaboration among EU member states, drawing in new players, especially SMEs, to penetrate the traditionally insular defense market.

The EDF is now the EU's second-largest defense research agency, supporting around 200 projects with over 1,000 beneficiaries. The program's structure ensures that topics for funding are defined by member states, aligning research efforts with actual defence needs and creating tangible business opportunities for participants. This strategic alignment not only enhances defence capabilities but also fosters a more competitive and integrated European defence industry.

European Defence Fund :
The E... Defence R&D prog
Support collabora... and ... border ... dis... tech...
Contribute to the competitiveness and innovation capacity of the EDTIB
Enco... partic... SMEs ... actors ... act... def...

EXPO STAGE, 20 JUNE

NEGOTIATING WITH CYBER CRIMINALS: LESSONS LEARNED FROM $100M RANSOMWARE CASES

During the presentation, **Azra Xheladini, Sales Manager for Europe** and **Burak Uyduran, Channel Marketing Manager at SOC RADAR**, explored the most significant ransomware attacks that have cost organisations billions. They analysed critical lessons learned from these high-stake incidents and provided insights to fortify defences against the ever-evolving ransomware threat landscape.

CYBERSEC EXPO & FORUM
SOCRadar
Your Eyes Beyond
Negotiating with Cyber Criminals
Lessons Learned from $100M Ransomware Cases
Azra Xheladini
Burak Uyduran

ARE YOU ABLE TO RECOGNISE A CYBERCRIMINAL IF THEY LOG IN WITH STOLEN CREDIDENTIALS? IDENTITY PROTECTION WILL ANSWER TO MODERN ATTACKS ON ACTIVE DIRECTORY

During the presentation, **Bartosz Galoch, CrowdStrike Product Manager at iIT Distribution Polska**, provided insights into the Crowdstrike Falcon platform, renowned as one of the world's most comprehensive solutions for safeguarding organisations from cybercriminals. He discussed strategies for combating the increasingly sophisticated and stealthy modern identity-based attacks targeting Active Directory (AD).

CYBERSECURITY OF OUTERSPACE

The presentation, led by **Andrea Lorenzini, Cyber-Security and Space Programme Accreditation Manager** at the European Space Agency, explored the growing reliance of critical infrastructure on space-based assets. It emphasised the need for robust security measures and highlighted the essential collaboration required across sectors to address the numerous vulnerabilities in the cyber resilience of outer space.

THANKS TO AI AND GENERATIVE AI, HOW TO DETECT THE NEW COMPLEX ATTACKS IN CRYPTED TRAFFICS, WHILE REDUCING THE BARRIER OF COMPLEXITY TO OPERATE A SOC

Dominique Meurisse, VP Sales International at Gatewatcher, stated that detection is a major issue in cyber security due to the complexity of recent attacks. It is important to detect cyber-attacks because an analysis of aggregations of incident logs is only valuable as a post-mortem tool. End-point protection is important because it reacts during an attack, but NDR or network detection response monitors the network in real time to detect early stages of an attack and mitigate emergencies. This is important because the quicker attacks are detected the better protected a business. Technologies often have security gaps, particularly if credentials have been stolen. ID violation has risen to prominence in recent years, as has ransomware attacks using data that was stolen early on in an attack. Stormshield combines technology and AI/LMs to increase known attack data, which decreases the complexity of a SOC. LMs are used to make a security playbook which uses company defence infrastructure, training data, and real time attack data in order to recommend best practises.

CYBERSECURITY WITHOUT COMPROMISE ON CONFIDENTIALITY. DEPLOYING A EUROPEAN EDR ON-PREMISE FOR PUBLIC AND SENSITIVE ORGANISATIONS

The presenter, **Tanguy Steeg, the Director of International Development**, introduced his company and their threat detection system. Mr Steeg highlighted that their system focuses on protecting both the Cloud and premise, as many sensitive organisations want to keep their information in a database. The speaker continued to break down how the program functions, by describing the agents at all end points which are trained to detect and block different types of attacks. All the data collected by the platform is then given to the company.

THE EUROPEAN CHOICEFOR CYBERSECURITY

The speaker, **Grzegorz Godlewski, Sales Manager of Poland at Stormshield**, started the presentation by providing a brief introduction into the solutions Stormshield delivers such as the deep package inspection which provides an analysis into things such as network security, industrial security, endpoint security and data security. Mr Godlewski then introduced the audience to the wide range of products which are utilized by both the civilian as well as the military sector. He explained the user-friendly aspect of the products by explaining in detail how they operate. The presentation was concluded by showing the various certifications of the products.

WHY IT GEEKS SUCK AT SELLING THEIR OWN BRILLIANCE: DIGITAL STRATEGY FOR CYBERSECURITY COMPANIES

The presentation, featuring **Paweł Kabata, CEO of Artixen.net**, and **Anna Nikiel, CEO of AiLead**, revealed common marketing and sales pitfalls that hinder IT and cybersecurity companies from realising their full potential. It introduced an efficient digital strategy aimed at boosting revenue by bridging the gap between technical proficiency and effective communication in the industry.

CHALLENGES OF CERTIFICATION FOR POLISH TECHNOLOGY COMPANIES

During a panel on the challenges of certification for Polish technology companies, **Elżbieta Andrukiewicz, Head of Cybersecurity Department, The National Institute of Telecommunications – the State Research Institute** highlighted the country's robust certification system, established between 2018 and 2022, which aligns with the Common Criteria agreement recognised globally by 34 countries. She emphasised Poland's unique position in the region with such a state program. **Paweł Kostkiewicz, Head of the Standardisation and Certification Centre at NASK** acknowledged the complexity and lengthy evaluation processes of certification projects, which limits the number of producers who ask for such certificates. Nevertheless, certificates are issued, two Polish companies – Asseco and Dynacon – were cited as examples.

Andrzej Dulka, President, Polish Chamber of Information Technology and Telecommunications, raised concerns about the high number of cyberattacks on Poland's telecommunications and information infrastructure, attributing many to state actors like Belarus, Russia, and North Korea aiming to disrupt national stability. Last year, there were around 300,000 incidents. **Sławomir Górniak, Senior Cybersecurity Expert, ENISA**, clarified that cybersecurity certification does not guarantee complete security but is meant to build trust that a product or service has been rigorously tested and meets specified standards. He explained that the European Cybersecurity Act aims to increase confidence in the security of certified products, processes, and services.

PANEL DISCUSSION, 11:00-11:40
CHALLENGES OF CERTIFICATION FOR POLISH TECHNOLOGY COMPANIES
Andrzej Dulka

Ms Andrukiewicz added that a program was developed to help Polish SMEs participate in certification programs, including detailed guidelines and cost calculations, but it has yet to be implemented. She emphasised that while large companies can afford certification costs, it remains a significant barrier for SMEs, especially those aiming to operate internationally, and expressed hope that Polish entrepreneurs will gain the skills and experience to achieve certification more easily in the future.

AI GOVERNANCE MODEL

In his keynote speech, **Matthias Muhlert, CISO, Oetker-Group** introduced his self-developed Governance Model for Artificial Intelligence, with a particular focus on Machine Learning. This model serves as a decision-making tool to determine whether AI should be utilised, rather than analysing its technical capabilities. The goal of the model is to have an AI decision model that fits on one single page, and is designed to assist various organisational stakeholders, including compliance, legal, and data privacy departments, in navigating the ethical, legal, and logical considerations of AI use. By providing a straightforward framework, Mr Muhlert's model helps demystify AI and ensures that the right questions are asked to understand potential risks and benefits.

PANEL DISCUSSION, 12:00-13:00
A COMPETENT COMMUNITY – A NEW FORM OF SYNER
IN EUROPEAN CYBERSECURITY ACTIVITIES
CYBERSEC

A COMPONTENT COMMUNITY – A NEW FORM OF SYNGERGY IN EUROPEAN CYBERSECURITY ACTIVITIES

During the discussion, **Michał Rekowski, Program Officer at ECCC** underscored that to tackle Europe's cybersecurity challenges, it's crucial to harness the collective strength of its many robust companies, innovative startups, and cutting-edge research centres. With a significant talent pool, particularly in Poland, the aim is to create a cohesive network that can compete globally against larger, better-funded adversaries. The EU's diversity is its strength, enabling complementary capabilities across the continent. **Andrzej Bartosiewicz, President of the CISO #Poland Foundation and founder of CISO4U** concurred with this sentiment, stating that sharing of ideas and best practises is crucial to European cyber security development, where a myriad of corporations of differing sizes face the challenge of breaking into a vast and competitive global market.

Echoing Rekowski's sentiments, other speakers elaborated on the multifaceted benefits of such a collaborative network. **Ewelina Kasprzyk, R&D& Specialist, AGH Cybersecurity Centre**, pointed out the crucial role of universities in providing not only education but also cutting-edge research and infrastructure to support technological advancements. **Zuzanna Wieczorek, CEO, Tekniska** and **Łukasz Gawron, President of the Board, Polish Cybercluster #CyberMadeInPoland**, stressed the importance of an active, inclusive community that bridges the gap between large and small enterprises, ensuring all voices are heard and all members can benefit from shared knowledge and resources. They advocated for a transparent, structured approach to foster collaboration and innovation, ultimately strengthening Europe's cybersecurity landscape and bolstering its global competitiveness.

HOW TO SECURELY DIGITALISE, AUTOMATE AND INNOVATE IN YOUR DIGITAL BUSINESS USING INTEGRATED TRUST SERVICES

In his presentation, **Edgars Stafeckis, CEO and Co-founder of TrustLynx**, highlighted the EU's Digital Single Market objectives, aiming for an ambitious 80% adoption rate of the EU digital wallet by 2030. Trust Lynx addresses critical challenges including data privacy, user adoption, and legal complexities through an integrated platform that ensures information security, privacy control, and tailored user experiences to meet specific business needs. Their solution streamlines automation processes for companies, facilitating secure interactions within controlled environments while adhering to regulatory standards and enhancing access to remote trust services at no cost to end-users.

COMPREHENSIVE RESPONSE TO CYBERSECURITY REQUIREMENTS

This presentation, led by **Krzysztof Sierański, CEO of Stillsec**, demonstrated the ongoing challenge of encountering several dozen vulnerabilities daily within organisations, which are increasingly complex. The approach to addressing these issues emphasises risk assessment, continuous monitoring, awareness building, incident response, and more.

DEMOCRATISING PRIVILEGED ACCESS MANAGEMENT (PAM) – CYBERSECURITY BEST PRACTISES FOR EVERYONE

Existing PAM solutions, while effective in mitigating many cyber attacks, often come with high costs and usability challenges. This presentation showcased Excalibur's innovative, user-friendly PAM solution, leveraging phone-based methods like peer verification and authentication to enhance cybersecurity, as presented by **Ivan Klimek, CEO and Founder of Excalibur**.

DEVELOPING IRELAND'S CYBERSECURITY ECOSYSTEM: LESSONS LEARNT AND CHALLENGES AHEAD

In his presentation **Bartosz Siepracki – Senior Market Adviser Digital Tech & High-Tech Construction at Enterprise Ireland**, covered the major stakeholders of the Irish cybersecurity ecosystem such as start-ups, government, academia, businesses and companies. He provided insight into the functions of some of these organisations, such as incident response and education, and highlights the role of investment into the skills of future cybersecurity professionals.

Kompleksowe rozwiązania cybersecurity dla bezpiecznego jutra
4Prime IT SECURITY
TestCLIX
SKYSEC

netia
netia next
SECURITY OPERATIONS CENTER

#CyberMadeInPoland
SOCRadar Your Eyes Beyond
EXTENDED THREAT INTELLIGENCE

axence

Elevate your security
our elite penetration tes
expertise
afine
digitally secure
VISIONCUBE

SIDE EVENTS AND SPECIAL FORMATS

ADMIN DAYS

On the first day of the CYBERSEC conference, the Admin Days workshops took place – one of the highest-rated series of events for the IT industry, organized by the Władcy Sieci portal and Axence. These are technical workshops focused on IT security and management, primarily aimed at administrators and cybersecurity specialists. Participants attended lectures and practical sessions, allowing them to expand their knowledge and exchange experiences with other industry experts. The event's agenda included best practices for IT departments in the context of NIS2 and practical sessions on analyzing cybersecurity incidents.

DYNACON WORKSHOPS

The Dynacon workshops, held on the first day of CYBERSEC CEE EXPO & FORUM, focused on the real reasons for the loss of operational continuity in OT domain systems, their monitoring, and response to threats. Led by Andrzej Cieślak, CEO of Dynacon, these workshops offered participants the opportunity to gain practical knowledge on building a comprehensive monitoring ecosystem, data analysis, threat identification, and preparing reactive measures for industrial environments. The workshop format included competitive elements, where participants tackled issues related to anomalies. The winning team was awarded professional courses with the opportunity to obtain NCSA certifications.

IRIS WORKSHOP

Organized during the 2nd day of the conference, the IRIS workshop provided an in-depth understanding of incident reporting complexities, the essential roles of Security Operations Centres (SOCs), and the benefits of cross-border information sharing. Participants explored AI and IoT threats and learnt about solutions for protecting critical infrastructure in smart cities. The H2020 IRIS project, aimed at preparing the EU industry for threats to IoT, ICS, AI, and other systems, was a focal point, showcasing a federated threat intelligence architecture with autonomous detection, privacy-aware intelligence sharing, and advanced data protection. Practical demonstrations were conducted in realistic smart city environments in Helsinki, Tallinn, and Barcelona.

CISO MEETING

On the 2nd day of the conference, **Dr. Andrzej Bartosiewicz, President of the CISO #Poland Foundation and Founder of CISO4U**, led the CISO #Poland Meeting. The guests discussed the risk and opportunities stemming from new and disruptive technologies, operational resilience and cyber threat landscape. The meeting was divided into three parts: #legislation, #transporation_UE and #quantum_computing & #artificial_intelligence. Among the speakers were Luigi Rebuffi, ECSO, Łukasz Wojewoda, Ministry of Digital Affairs, Piotr Józefczyk, Group CISO, Raben and Arkadiusz Osypiuk, CISO #Poland, Chairman CISO #Poland #AI.

CEE ROUNDTABLE

Organized by the Digital Poland Association and CEE Digital Coalition and Lead by **Michał Kanownik, President of Digital Poland Association (ZIPSEE)**, this roundtable brought together representatives from the CEE regions to discuss the current state of CEE cybersecurity cooperation and provide recommendations on how to strengthen such collaboration. During the Roundtable, the **Deputy Prime Minister, Minister of Digital Affairs, Krzysztof Gawkowski**, gave a keynote speech.

IRIS 3RD STAKEHOLDERS AND INDUSTRIAL WORKSHOP

The second workshop organized by IRIS consortium was aiming to give the participants a chance to watch demonstrations of the project's solutions and tools and connect with industry professionals, stakeholders and experts in a hybrid setting.

CYBER FORTRESS

The 5th Tournament of the 4th Season of the Cyber Fortress League was held on the first day of the event. "Cyber Fortress" is a simulation game of building the most resilient security system for the ICT environment and responding effectively to various cyber threats. In Cyber Fortress the participants could play out a scenario based on real incidents observed in cyberspace. During the event, the participants had a chance to play out a scenario based on real incidents observed in cyberspace, which related to real cases.

CYBER TRAINESS

The Kościuszko Institute actively supports educational and professional initiatives aimed at supporting women in the field of ICT and cyber. During this year's edition of CYBERSEC we have the opportunity to complete the second edition of Cyber Trainees – an educational course coordinated by the Kosciuszko Institute as part of a grant awarded by the Microsoft Foundation. The goal of the course is to increase the inclusiveness of the ICT market for women.

After nine months of intensive study during weekend classes, almost 60 women from all over Poland completed the course, and some of them managed to attend the official graduation ceremony during the CYBERSEC CEE EXPO & FORUM conference in Krakow. On site, Ladies had the opportunity to listen to discussion panels and presentations, as well as participate in joint networking.

At the graduation we had the pleasure of hosting a representative of Microsoft, **Nikolas Ott Senior Manager, European Government Affairs**, but also representatives of the course's Meritorical Partner: **testuj.pl, Test Army**, as well as the Supporting Partners: **EY Academy of Business** and **Kyndryl**.

As a result of two editions of the Cyber Trainees project led by **Karolina Wojtyczek, Project Manager of the Kosciuszko Institute**, over 130 women (Polish and Ukrainian) have completed the course and started their adventure in the cyber security sector.

#CYBERMADEINPOLAND ZONE

#CyberMadeInPoland Zone was a special space dedicated to companies gathered in Polish Cybersecurity Cluster. 18 polish companies during the two-day event had the opportunity to present their products and services.

In the #CyberMadeInPoland Zone you were able to find:

- Afine
- Axence
- CDeX
- CyCommSec
- Dynacon
- Perceptus
- SISOF
- Test Army
- IDENTT
- Cryptomage
- Atende
- DEKRA Certification
- Artixen.net
- Rublon
- Resilia
- ChangePro
- StillSec
- Xopero Software

Ekran system
SECURIV
Odwiedź naszą Stronę
ROAD TO THE POLISH PRESIDENCY 2025 - CYBERSECURITY PRIORITIES FOR EUROPE

AMONG CYBERSEC CEE EXPO & FORUM 2024 GUEST SPEAKERS

KRZYSZTOF GAWKOWSKI
Deputy Prime Minister,
Minister of Digital Affairs

LUCA TAGLIARETTI
Executive Director, ECCC

ŁUKASZ SĘK
Deputy Mayor of City Kraków

COL. JAROSŁAW WACKO
Lead Specialist, Polish Cyber Command

CHRISTIANE KIRKETERP DE VIRON
Head of Unit for Cybersecurity and Digital Privacy,
DG CONNECT, European Commission

TADEUSZ CHOMICKI
Ambassador for Cyber & Tech Affairs, Polish Ministry of Foreign Affairs

TERESA RIBEIRO
Representative on Freedom of the Media, OSCE

MIGUEL ANGEL CAÑADA
Head of the National Coordination Center (NCC-ES INCIBE) of the Spanish National Cybersecurity Institute

LISE FUHR
Director General, European Telecommunications Network Operators' Association (ETNO)

KATARZYNA PRUSAK-GÓRNIAK
Head of Digital Unit
at the Permanent Representation
of the Republic of Poland
to the EU

AXEL DEININGER
Chairperson, ECSO

PROF DR PAUL TIMMERS
Research Associate, University of Oxford

AMONG CYBERSEC CEE EXPO & FORUM 2024 GUEST SPEAKERS

JÓZEF GAWRON
The Deputy Marshal
of the Małopolska Region

INGRIDA TAURINA
Head of Executive Director's
Office, ENISA

MATTHIAS MUHLERT
CISO, Oetker-Group

COMMANDER DAVIDE GIOVANNELLI
Law Researcher at the Law
Branch of the NATO
Cooperative Cyber Defence
Centre for Excellence
(CCDCOE)

JOANNA ŚWIĄTKOWSKA
Deputy Secretary-General,
European Cyber Security
Organisation (ECSO)

MARC VANCOPPENOLLE
VP Government Affairs EU
& Europe, Nokia

FLORIAN PENNINGS
Director European Cybersecurity
Policy, Microsoft

YANN BONNET
Deputy CEO of Campus Cyber

MAJOR GENERAL JEAN-MARC WASIELEWSKI
Retired Major General, Signal
Corps of the French Army

DAVID ANTUNES
Cyber Defence Programme
Manager, European Defence
Agency

DR INŻ. ANDRZEJ BARTOSIEWICZ
President of the CISO #Poland
Foundation and Founder
of CISO4U

ANDREA LORENZINI
Cybersecurity & Space
Programme Security
Accreditation Manager at the
European Space Agency

CYBERSEC CEE EXPO & FORUM 2024 PARTNERS

STRATEGIC PARTNER

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

MAIN PARTNER

MAŁOPOLSKA

HOST CITY

Kraków

PLATINUM PARTNER

Microsoft

GOLD PARTNERS

CAMPUS CYBER

IBM®

CYBERSEC CEE EXPO & FORUM 2024 PARTNERS

SILVER PARTNERS

CROWDSTRIKE
NOKIA
stillsec
4Prime IT SECURITY
afine digitally secure
SOC360 CYBERSECURITY
DYNACON Connecting Data
axence
VISIONCUBE
ALIOR BANK
SOCRadar Your Eyes Beyond
iiTD INTELLIGENT IT DISTRIBUTION
Enterprise Ireland

EXHIBITORS

ECSO EUROPEAN CYBER SECURITY ORGANISATION
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
NCC-PL National Cybersecurity Coordination Centre Poland
MAŁOPOLSKA
Microsoft
CYBER COMMAND POLAND
CROWDSTRIKE
CAMPUS CYBER
GATEWATCHER
HarfangLab
seclab
STORMSHIELD
Ekran system
SECURIVY
BlackBerry Cybersecurity
SiSOFT
CYCOMMSEC
SECTRA
Kingston TECHNOLOGY
TestArmy
testuj.pl szkolenia dla firm

EXHIBITORS

#Cyber Made InPoland
perceptus
WEDOS
4Prime IT SECURITY
afine digitally secure
SOC360 CYBERSECURITY
SKYSEC IT Auditors
TestCLIX
isperia
TRUST LINX
stillsec
FBI Polska
advatech
CDEX
DYNACON Connecting Data
axence
XOPERO Backup&Recovery
cynet
ISCG
MAXTOOLS Future is Possible
VISIONCUBE
greeneris
zscaler
Excalibur
DEKRA

EXHIBITORS

Resilia business resilience architects
Rublon
GET3S FOUNDATION
ab systems WE DO IT
Enterprise Ireland
IDENTT
cryptomage
ATENDE
PAESSLER THE MONITORING EXPERTS
iiTD INTELLIGENT IT DISTRIBUTION
SOCRadar Your Eyes Beyond
Green Cell
KRYNICZANKA
netianext
iRiS
boat.systems
EY Academy of Business
bako tech
matrix INTERNET
Stryve
TitanHQ
GETVISIBILITY own your data
ARTIXEN.NET TWORZYMY INTERNET
AILEAD
ChangePro CYBERSECURITY AWARENESS COMPANY
ARCHER

CYBERSEC CEE EXPO & FORUM 2024 PARTNERS

COMMUNITY PARTNERS

techies SPACE powered by CODETE

justjoin.it

geekweek

Green Cell

UZDROWISKO KRYNICA-ŻEGIESTÓW S.A. 1793 KRYNICZANKA

HONORARY PATRONS

Minister of Digital Affairs Republic of Poland

Minister of Foreign Affairs Republic of Poland

Ministerstwo Obrony Narodowej

Ministry of Economic Development and Technology Republic of Poland

MAŁOPOLSKA MARSHAL OF THE MAŁOPOLSKA REGION

EUROPEAN DEFENCE AGENCY

CCDCOE

under the patronage of the European Parliament

Kraków

BBN BIURO BEZPIECZEŃSTWA NARODOWEGO

CENTRUM PROJEKTÓW POLSKA CYFROWA

PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

iab polska 25

Polish Investment & Trade Agency PFR Group

PARP Grupa PFR

RCB

NCBR National Centre for Research and Development

UKE Office of Electronic Communications

AGH University of Krakow AGH

PIIT

Instytut Łączności

INSTITUTIONAL PARTNERS

A-SIT

Polska Chmura

ICANN

ISACA Warsaw Chapter

KRAKOWSKI PARK TECHNOLOGICZNY

INSTITUTE OF NEW EUROPE

ESI European Software Institute Center Eastern Europe

Polish Platform For Homeland Security

DEMAGOG

Łukasiewicz Instytut Technik Innowacyjnych EMAG

SecOps POLSKA

SysOps/DevOps Polska

IIAW Instytut Audytorów Wewnętrznych IIA Polska

ECCC

CyAN Cybersecurity Advisors Network

PIIT

University of Economics in Katowice

17 53c

STARTUP HUB POLAND

DIGITALEUROPE

Perspektywy WOMEN IN TECH

CENTRUM CYBERBEZPIECZEŃSTWA AGH

WOMEN 4CYBER POLAND

BYDGOSKI KLASTER INFORMATYCZNY

FUNDACJA bezpieczna cyberprzestrzeń

Business France

vestbee

CYFROWA POLSKA

MEDIA PATRONS

DGP Dziennik Gazeta Prawna

FORSAL.PL

sekurak.pl

securITum

security magazine

CyberDefence24

radio eska

eska2

POLSKA PRESS GRUPA

Strefa Biznesu

i.PL

Gazeta Krakowska

NEWSERIA AGENCJA INFORMACYJNA

NEWSERIA BIZNES

NEWSERIA INNOWACJE

CYBERSEC
EXPO & FORUM

CYBERSEC EXPO & FORUM
19-20 JUNE 2024
MAŁOPOLSKA
MAIN PARTNER
PANEL DISCUSSION, 10:30-11:30
ROAD TO THE POLISH PRESIDENCY 2
CYBERSECURITY PRIORITIES FOR EU
Axel Deininger
Miguel Angel Cañada

NEXT CYBERSEC CEE EXPO & FORUM IN 2025!

INTELLIGENT IT DISTRIBUTION
Jesteśmy specjalistycznym dystrybutorem z wartością dodaną (Value Added Distributo oferującym kompleksowe rozwiązania z zak bezpieczeństwa informacji i cyberbezpieczeństwa.
WWW.ACSG.EDU.PL
DYNACON