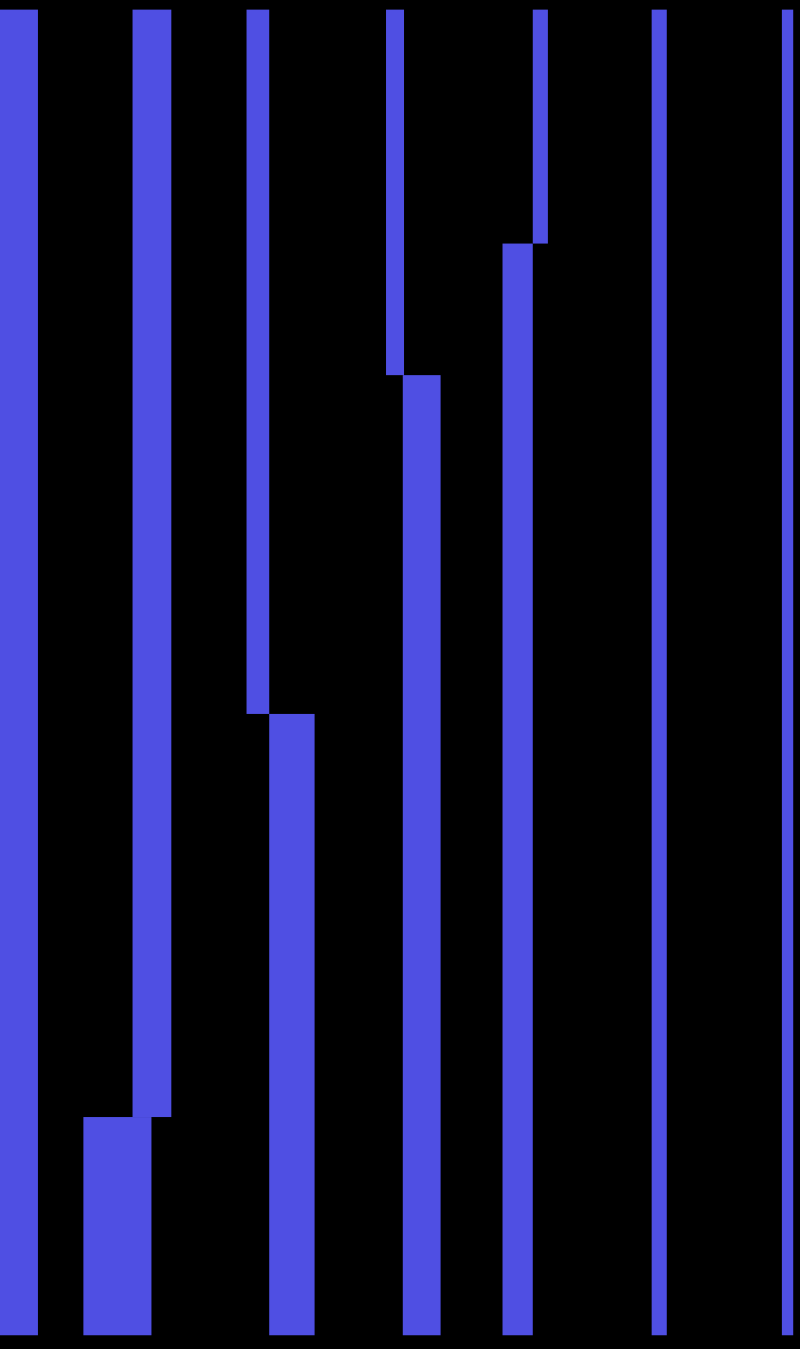
INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

AUSTRIAN INSTITUTE OF TECHNOLOGY

WKO AUSSENWIRTSCHAFT AUSTRIA

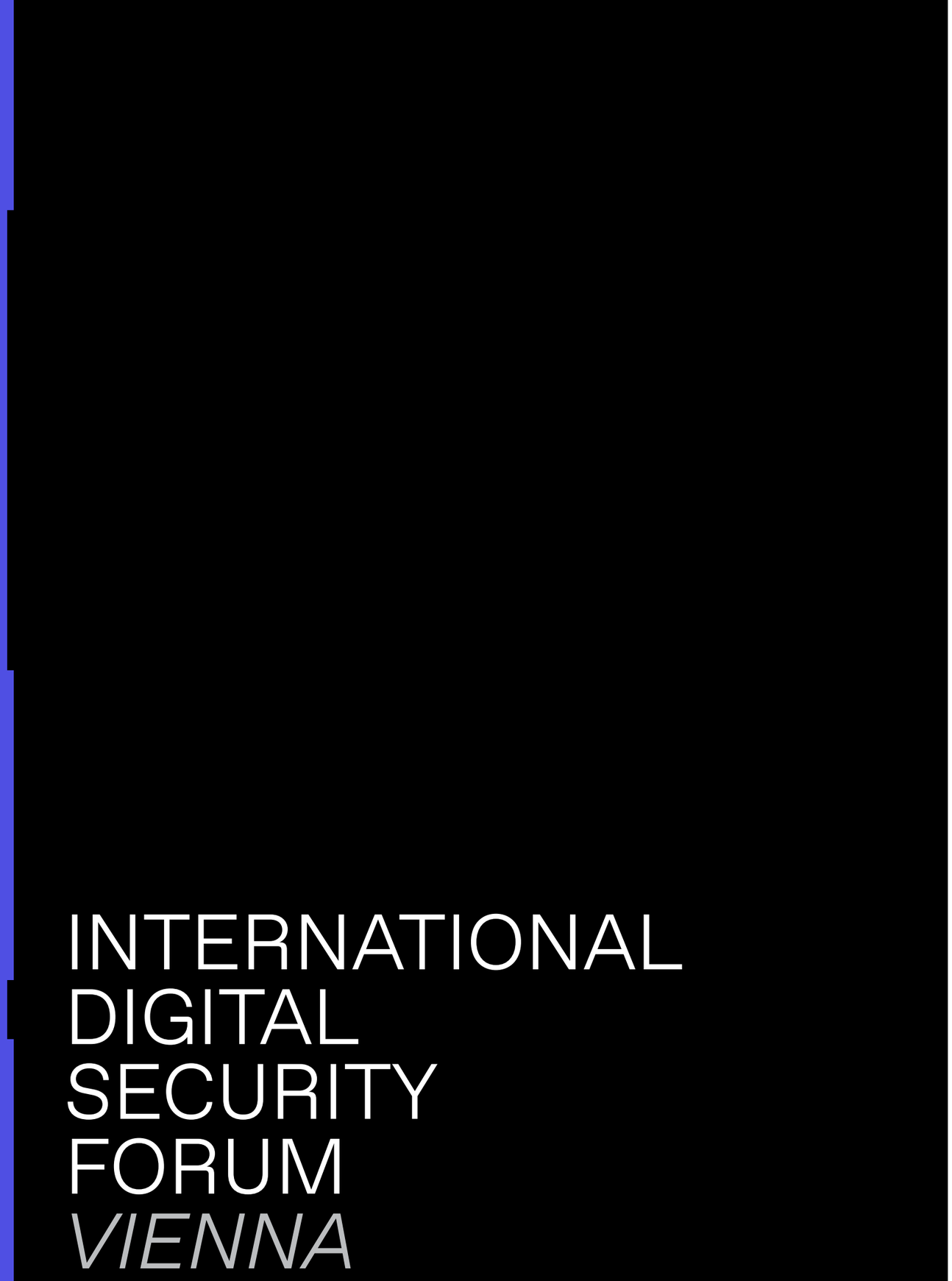
go international

Bundesministerium Digitalisierung und Wirtschaftsstandort



Security in times of pandemic and major global events

CONFERENCE REVIEW 2020



Overview

Security in times of pandemic and major global events

2. – 3. December 2020

The novel Coronavirus (COVID-19) has led to challenges and chaos to many aspects of life. It is hard to imagine a sector of society that has not been somehow impacted and will continue to be for an extended period of time. During this period and the recovery period, technology has been a major facilitator for understanding and tracking the pandemics, but also in allowing a level of remote presence for both work and social engagement.

“Work from Home” has become the norm for many. The International Digital Security Forum (IDSF) seeks to bring together international and national leadership and stakeholders in information exchange and collaboration. The goal is to build collective knowledge of lessons learned and to build partnership for pandemic and major event mitigation.

Under the motto “Global Discussion for a Connected World”, the IDSF 2020 was organized as a virtual conference from 2–3 December 2020 by the AIT Austrian Institute for Technology and the Austrian Chamber of Commerce (Wirtschaftskammer Österreich – WKO).

DAY 1

Welcome & Opening Session

9 Mariana Kühnel (Conference Host)

10 Christian Weissenburger
11 Margarete Schramböck
13 Sebastian Kurz

15 Vladimir Voronkov (Keynote)

Fake News – Undermining Democracy

17 Dominika Hajdu, Miroslawa Sawiris, Laura Loguercio, Caroline Schmidt, Andy Stoycheff & Ross King (Host)

Fake News – The New Role of Media

21 Wolfgang Renner (Host), Katharina Schell, Nikos Sarris

Austria in Security Research – The Digital Dimension

23 Andreas Reichhardt (Keynote)

An African Perspective on Digitalization

25 Hon. Vincent Waiswa Bagiire, Philipp Agathonos (Moderator)

2. December 2020

Digital Resilience & Complexity

26 Alexander Schatten (Host), Lukas Feiler, Andreas Windisch

Next Generation Border Management

31 Giulio M. Mancini, Romain Nivelle, Georgios Boultadakis, James Ferryman, Pantelis Michalis, Andreas Kriechbaum-Zabini (Host)

Advanced Biometrics for Counter Terrorism

35 Nelson Goncalves, Reinhard Schmid, Andreas Wolf, Rocco Messina, Margherita Natali, Bernhard Strobl (Host)

Women in Cyber-Security

36 Chris Ensor, Zoe Edmeades, Sayako Qinlan)

New Rules for Economic and Cyber Security

37 Mika Lauhde

3. December 2020

Welcome & Opening Session

39 Karl Nehammer

40 Arne Schönbohm (Keynote)

Challenges and Abuse of Virtual Currencies

43 Rainer Böhme, Haaroon Yousaf, Georgios Kappos, Eljo Haspels, Kamal Anwar, Bernhard Haslhofer (Host)

Trust in Complex Cyber-Physical Environments

44 Mario Drobics, Stefan Mangard, Philipe Reinisch, Julia Pammer

Explainable AI

46 Sepp Hochreiter, Allan Hanbury, Jochen Borenich, Mariarosaria Taddeo, Willibald Krenn (Host)

Next Generation Situational Awareness Systems

49 Georg Aumayr, Harald Felgenhauer, Christian Resch, Niek Mestrum, Marcel Van Berio, Karin Rainer, Georg Neubauer (Host)

DAY 2

From Automated Data Analysis to Mobile Fingerprinting

50 Joachim Müller, Gareth Balance, Jürgen Mathwich

Cyber Security – Capability Building in Times of Covid

51 Bernd Pichlmayer, Trent Nelson, Álvaro de Lossada Torres-Quevedo, Alexander Janda, Thomas Braun, Donald Dudenhoeffer (Host)

Cyber Security – Technology and Security in the Age of Pandemic

54 Friedrich Teichmann, Fernando Puerto Mendoza, Kai Rannenberg, Rafal Jaczynski, Arne Schönbohm, Marie-Line Billaudaz, Gert Seidl, Helmut Leopold (Host)

A GLOBAL DIALOGUE FORUM FOR SECURE DIGITALISATION – NOW MORE IMPORTANT THAN EVER

Helmut LEOPOLD, PhD
Initiator of IDSF Vienna & Head of
Center for Digital Safety & Security, AIT
Austrian Institute of Technology

Michael MÜRLING
Head of IDSF Organisation & Science
Communicator at Center for Digital
Safety & Security, AIT Austrian
Institute of Technology

PREFACE

For the first time in human history, digitalisation and global networking have created entirely new ways of interacting, and opened up almost limitless and universal access to the world's knowledge. Today's information and communication technologies are the product of an unparalleled transformation, which has had a global and substantive impact on society and become the backbone for all areas of our lives. We need new skills, digital tools and sustainable infrastructures to address and respond to major societal issues in the fields of energy, healthcare, transport management, environmental and climate change management, and to find solutions to the growing challenges emerging in the security sector, including crisis and disaster management, border management, the fight against terrorism, the protection of critical infrastructures, secure smart cities as well as detection of disinformation, which is vital for sustaining a democratic society.

To give one example, social media is the largest and most powerful communications mechanism we have ever created, allowing both emotional and polarising messages, as well as simply false information, to be easily generated and shared. Social media has caused entire social groups and societies to be deliberately alienated and even manipulated. When such deliberate disinformation is combined with targeted cyber-attacks on critical infrastructures or public authorities, we talk of 'hybrid threats'. Ultimately, these can be used to threaten entire states, and shake the very foundations of our democracy.

This radical transformation has impacted all the economic and social areas of our lives. At the same time, we have all become dependent on these technology platforms to the extent that a flourishing economy, a prosperous society, and functioning state institutions, as well as an established democracy, are all unthinkable without perfectly functioning digital infrastructures. The coronavirus pandemic has made this very clear indeed.

Therefore, as digitalisation continues to develop rapidly, it is essential that all stakeholders in science and research, industry, as well as the public authorities, cooperate effectively to jointly master the challenges that global digitalisation brings. This requires three essential conditions:

1. All stakeholders must ensure continuous technology management and maintain their ability to act autonomously.
2. Ongoing and close cooperation between public authorities and research bodies must be established to develop suitable framework conditions as well as effective and targeted protective mechanisms in the course of digital technology developments.

3. In view of the extremely short innovation cycles of digital technology, public authorities must be aware of the need to establish the necessary competences and skills in good time so that effective digitalisation processes can be supported over the long term.

In light of sweeping, global digitalisation, in 2020 a new international dialogue format was created – IDSF, the International Digital Security Forum. It is designed to allow security sector stakeholders from around the world to come together to talk openly, to learn from one another, to share knowledge, and to create the framework conditions which – in a constant race against the latest threats – allow them to jointly ensure the best possible level of protection for our vital digital infrastructures and applications. For that reason, we have adopted a holistic approach which allows us to deliberately focus on the most pressing digital security issues.

At the first IDSF forum, in December 2020, these issues included cyber security, digitalisation in the field of border management, the fight against terrorism and cybercrime, as well as measures to control the abuse of cryptocurrencies. The growing phenomenon of fake news and the use of explainable artificial intelligence were also on the international discussion agenda. At the meta level, the experts at the conference explored strategic options for developing better systems for active awareness of threat scenarios, and to strengthen the international resilience of complex digital systems by jointly building up knowledge.

In this respect, special thanks go to the Austrian Ministries for their support. IDSF has allowed Vienna to position itself as a centre for global digitalisation dialogue. We are also grateful to the high-ranking representatives from major global and European organisations including the UN, IAEA, the German Federal Office for Information Security (BSI), the Goethe University Frankfurt in Germany, the Oxford Internet Institute, Globesec Bratislava, the SOMA Institute, and EDMO, as well as representatives from Africa and Asia, whose stimulating discussions all contributed to the success of the first IDSF.
Due to the pandemic, the first IDSF was held in the form of a hybrid conference, with most of the sessions run virtually. This faced us, the organisers, together with WKO ADVANTAGE AUSTRIA and technical partners including TVSalon, with a completely new set of challenges which are now part of modern event management. There was also an online exhibition for companies in the digital security industry which ran parallel to the presentation sessions.

We would like to take this opportunity to thank all the Austrian Ministries who were involved in the event, our sponsors, media partners and exhibitors, as well as our moderator Martin Szelgrad, for supporting the more than 500 visitors who took part in the 2-day conference programme. It is due to these partners and their enthusiastic input that it was possible to make the IDSF a success in this format.

We hope that those of you reading this brochure, which documents the forum proceedings, will either be pleasantly reminded of the stimulating talks and discussions you attended, or – for those of you who were not able to take part in December 2020 – that you will discover plenty about the fascinating world of digital security.

As the initiators and organisers of the IDSF, we are proud that the event has helped raise awareness of Austria and its capital as a digital security hotspot among a global audience. And, just as with all major events, the next IDSF is already in the planning stages – we will return with the second edition of this international event in Spring 2022.

WELCOME & OPENING SESSION

WELCOME
02.12.2020

Mariana Kühnel

Deputy Secretary General of
the Austrian Federal Economic
Chamber (WKO), Conference Host

© WKÖ / Nadine Studeny

Marina Kühnel regretted that the pandemic had prevented the ‘come together’ at the first IDSF from being face-to-face, but noted that the virtual format was highly appropriate for discussing the subject of cyber security. She felt that cyber security has gained in significance during this ongoing crisis. Cyber security was now more than just digital resilience, the fight against cyber crime, and the challenge of dealing with fake news, instead also becoming a factor which ensures that we can all move freely in virtual space without the risk of infection.

For Kühnel, the Corona crisis has indisputably triggered the biggest global economic crisis of recent years, and many of its consequences are not yet known. At the same time, the lockdown has demonstrated the role of digitalisation, and how this has become more important over time. Kühnel made a clear comparison: digitalisation is like a vaccine against the crisis.

In her view, digitalisation enables people, as well as companies, to stay connected in these challenging times, as well as to create innovations and channels which allow them to remain in constant contact with their customers and partners.

It is clear to her that digitalisation brings both opportunities and challenges – digitalisation always comes with the risk of cyber attacks and data leaks, which we must deal with.

Kühnel clearly stated that digital security is not only about technology, but primarily about individuals, with awareness being the key factor in establishing an effective ‘human firewall’. The human-technology interface is one of the areas of greatest risk, one we need to work on and increase awareness of.

In Kühnel’s eyes, events such as IDSF are important because they focus on encouraging international exchange and present cyber security as a key issue of our modern age. As a senior representative of the WKO, co-organiser of the event, Kühnel was delighted to welcome the several hundred participants who were joining from all over the world to listen and talk with experts.

Kühnel concluded her welcome address by wishing everyone an exciting conference experience, the fruitful exchanges of new ideas, and fresh leads for businesses and organisations. The carefully chosen format would ensure the health and safety of attendees. She closed with the plea: “Please remember that, although born of necessity, digitalisation can definitely be a virtue.”

WELCOME
02.12.2020

Christian Weissenburger

Director General at the Federal Ministry for Climate Protection, Environment, Energy, Mobility, Innovation and Technology, on behalf of Federal Minister Leonore Gewessler

© BMK/ Johannes Zinner

Ladies and Gentlemen!

On behalf of Ms Leonore Gewessler, Minister for Climate Action, Environment, Energy, Mobility, Innovation and Technology, it is a great honour for me to welcome you to the International Digital Security Forum 2020.

In the following two days representatives of organisations and high ranking speakers and panellists will discuss important topics in many fields of digitalisation.

Austria has, not least thanks to the valuable contribution of the Austrian Institute of Technology, an important role in many fields of the respective research and the development of technologies.

Digitalisation is the application and the transformational use of digital technologies.

It is one of the greatest engines for the development of our economy, and one of the major influencing factors in almost all aspects of society and personal life.

As a prime example, we only need to look at our current pandemic experience. Imagine the situation today if there were no digital technologies, no internet, no smartphones. There would have been a complete economic collapse.

In businesses as well as in our personal lives, we are constantly confronted with many new digital technologies and their applications. Artificial intelligence, cyber security, blockchain, the internet of things, 5G, have all become constants in our life. Likewise, new technologies continue to emerge on a nearly daily basis.

In the development of new digital technologies, it is critically important to recognise that technology is not an end in itself, but it is a tool that must serve and support people and processes.

True transformation results from the interaction between people and technology. It is essential that we develop suitable framework conditions for new technology integration and use.

The consequence of failing to develop such a framework ranges from potential monopolisation by global corporations to adverse safety and security conditions resulting from careless human use or malicious acts.

Effective governance in the form of

- standards
- effective laws and regulations
- and a code of ethics

is needed for the many aspects of digitalisation and the integration of new technologies as effective tools for business, industry, and society. Furthermore, this needs to be a global dialogue as technology knows few borders.

The International Digital Security Forum (IDSF) brings together digital experts, scientists, researchers, both national and international competent authorities, and business stakeholders from around the world to Austria.

We come together to share experiences, exchange knowledge, and to learn from each other with the goal to expand global knowledge in this comprehensive area. We will discuss the development and usage of new digital technologies such as

- cyber security,
- trust & ethics in AI,
- use of biometric data,
- and fighting against fake news and disinformation

among others to shape a technology that really supports our needs as end users.

Open discussion between the array of stakeholders in a global context is an absolute condition to support considerations and decision making regarding the emergence and integration of new technology into business, industry, and society.

Austria
- as the home to many international organisations,
- with its high tech industry,
- and internationally known research facilities,

welcomes the opportunity to hold this forum and lead this very important global discussion on digital transformation and associated security considerations.

I would like to thank the AIT Austrian Institute of Technology and the Austrian Federal Economic Chamber (WKO) as well as all organisations and companies for their commitment and contribution to the organisation of this global conference in Austria.

As Austria's Ministry for Innovation and Technology, we are very interested in the outcome and the findings of this conference; they will be a valuable contribution to our work and to the cooperation between state entities and science.

I wish everyone great success in the following days.

WELCOME
02.12.2020

Margarete Schramböck

Federal Minister for Digital and Economic Affairs

© BMDW/Hartberger

Federal Minister Margarete Schramböck was delighted to attend the IDSF because, in her view, the ongoing COVID-19 crisis makes it necessary for events to enter the digital space. She was also convinced that the shift to online interaction works extremely well, for all of us, both in our private and professional lives. This gives cyber security an important role, even more so as a result of the Corona crisis. Working from home and home schooling offer many opportunities for hackers, and companies are no longer as safe as they once were. We now need the right solutions in place to address these problems, Minister Schramböck, noted.

She is also convinced that digitalisation is essential for any digitalised administration and its various offices that wishes to provide its citizens and businesses with secure public services, both simply and 24/365. As an example, the Minister referred to the go-international network, operated by her Ministry in cooperation with the Austrian Economic Chamber, which is available digitally to companies during Corona times. The network assists companies in expanding their international footprint and conquering distant markets. This initiative also helps Austrian cyber security companies to position their products and solutions in foreign markets.

Schramböck also noted that, when it comes to digitalisation, there is an observable shift in mindset amongst small and medium-sized Austrian enterprises, which represent 98% of the country's entrepreneurs. Until recently, many companies saw no great need for digitalisation, whereas now 92% understand that they need to work on this transformation.

In her welcome address, the Minister noted the two main advantages offered by digitalisation, namely the modernizing and speeding-up of internal processes, and establishing new business models, for example, in the field of e-commerce. But these solutions must be secure. This means they must not only comply with the European GDPR, but also protect each company's assets. Another key goal of cyber security is to avoid long and costly operational downtimes following cyber attacks.

For Minister Margarete Schramböck, the last piece in the digital puzzle is education. We should drive digital education and develop training modules on cyber security which should then become an integral part of all apprenticeships in Austria. Schramböck is in no doubt that understanding digitalization and cyber security should not just be the preserve of experts, but instead part of every employee's standard set of working skills. These skills have never been more important than they are today.

Schramböck closed by wishing all the attendees an enjoyable Forum, the chance to gain valuable insights and make useful contacts, and to stay safe and healthy.

WELCOME & OPENING SESSION

WELCOME
02.12.2020

Sebastian Kurz

Federal Chancellor of the Republic of Austria

© BKA/Jakob Glaser

Dear Ladies and Gentlemen,

it is a pleasure to welcome all of you – this year digitally via live-stream – to the International Digital Security Forum in Vienna.

The ongoing pandemic has shown to all of us how far digitalisation has come in the last years and how important it will be going forward. Home schooling, managing medical resources or staying close in times of social distancing – in all these areas, digitalisation plays an important role in tackling the COVID-19 crisis successfully.

But the crisis has also revealed the challenges that we are facing in this field: the dependency on technology from limited suppliers, the clash of the cloud and data protection laws, and the increasing threat of fake and manipulated information.

Maintaining digital sovereignty is probably one of the most ambitious priorities for every government in the 21st century.

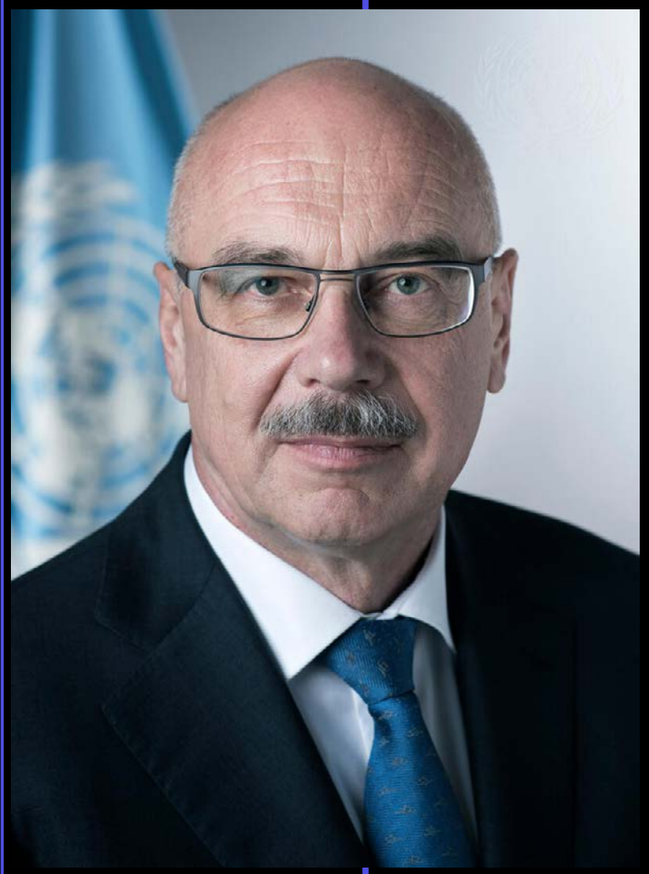
I'm glad that the Austrian Institute of Technology, in cooperation with the Austrian Federal Economic Chamber, has established this forum to openly discuss economic and social aspects of new technologies, to compare approaches from all over the world, and to work on the establishment of global digital values in times of digital change.

I wish you interesting presentations, successful discussions and hope to see all of you in person in Vienna next year.

Keynote

Vladimir Voronkov

Under-Secretary-General
United Nations Office of Counter-Terrorism
Executive Director, United Nations Counter-Terrorism Centre (UNCCT)



© UN Photo/Mark Garten

Excellencies, Ladies and Gentlemen,

Allow me to begin by thanking the Austrian Institute of Technology (AIT) for inviting me to address you at the opening of the 2020 International Digital Security Forum.

I would like to express to our Austrian hosts and friends my sincere condolences for the recent attacks in Vienna, a city that means so much to me, and my heartfelt solidarity with the victims and their loved ones.

Excellencies, Ladies and Gentlemen,

All of you attending today are doing important work on the most pressing issues regarding security and the use of technologies. And all of you, I am sure, have had to adjust your work to the limitations caused by the COVID-19 pandemic.

We were all already heavily dependent on information technology in our work, but now our use of it is constant and the need for digital security has multiplied.

Our own UN-way of working has had to adapt to this new reality.

In July, the United Nations Office of Counter-Terrorism successfully organised the first ever Virtual Counter-Terrorism Week. Over 1,000 people from 134 countries participated in its interactive discussions.

The event underlined the importance of maintaining our collective vigilance against terrorists and violent extremists in a pandemic context, as well as the need to reinvigorate multilateralism in the fight against this global scourge.

During the Virtual Counter-Terrorism Week we also launched an online exhibition about the work of the United Nations Counter-Terrorism Centre in the UN Office of Counter-Terrorism. I encourage you all to visit the UNCCT Expo, which remains available on our website, and represents a significant example of our new way of working online.

Over the past two years, UNCCT and the Austrian Institute of Technology have closely worked together on issues such as cyber security, artificial intelligence and the responsible use of biometric systems in the context of border security and management.

This included the joint organisation of the Global Innovation Challenge—or hackathon—on Countering Digital Terrorism, which the AIT hosted in Vienna in December 2019.

During the hackathon we brought 13 teams of young innovators from across the world to Vienna to present their creative solutions.

I hope we can continue this wonderful engagement with youth as we jointly address digital security. Young people have an inherent understanding of some of the key counter-terrorism issues, and great ideas to solve them.

During 2020 AIT and UNCCT strengthened their cooperation on the use of contactless biometric technologies and advanced biometric systems for identity document verification in the context of border security.

Both the United Nations and AIT recognise that biometric identification is an effective and powerful tool for Member States to responsibly and properly identify terrorists, in compliance with the requirements established by UN Security Council resolution 2396 and human rights.

While my Office works with Member States to promote the use of innovative technologies to counter terrorism, we are aware of the serious risks that come along with many of these tools.

Technologies such as biometrics, cryptocurrencies, social media and AI systems, can create significant legal, security and public health challenges.

To address them, it is critical that we develop comprehensive and human rights-sensitive approaches, share good practices, and foster public-private partnerships.

Excellencies, ladies and gentlemen,

COVID-19 is testing national and international resilience as well as global solidarity. This pandemic has the potential to exacerbate grievances, undermine social cohesion and fuel conflict, creating conditions conducive to the spread of terrorism.

Terrorists are exploiting the disruption, uncertainty and economic hardships caused by COVID-19 to spread fear, hate and division and radicalise and recruit new followers.

They are particularly targeting young people, who have been hardest hit by the wide-ranging social and economic impacts of the virus, and can be easily targeted by terrorist groups through the use of new technologies.

Deadly global threats such as terrorism and COVID-19 require us to act together, with a renewed sense of solidarity.
As Secretary-General António Guterres noted when marking the 75th Anniversary of the United Nations in September: "Today, we have a surplus of multilateral challenges and a deficit of multilateral solutions."

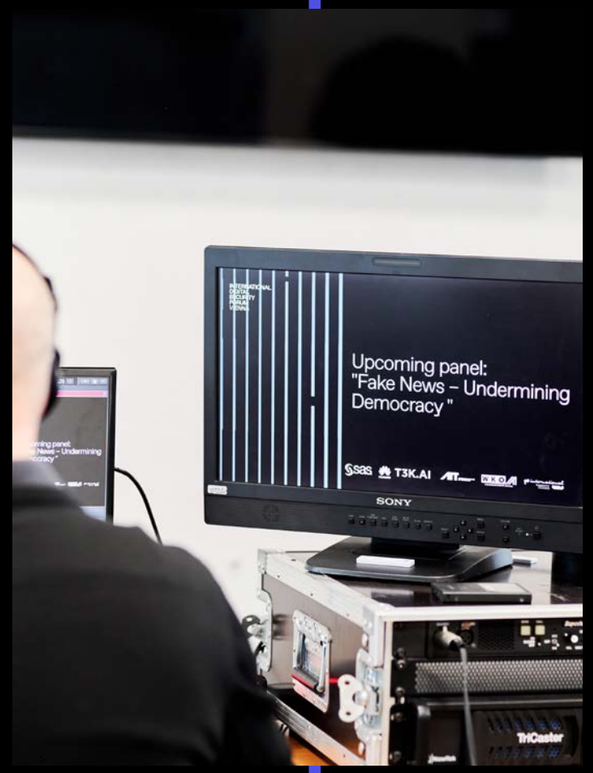
This is why your discussions over these two days are so important: only through cooperation and common understanding of our challenges and priorities will we be able to leverage technology to better face global threats and security risks.

I wish you fruitful discussions during the Forum, with the hope that next year we will all meet face-to-face.

Vielen Dank!

FAKE NEWS –

Undermining Democracy



Speakers

Dominika Hajdu
Research Fellow at GLOBSEC Bratislava

Miroslawa Sawiris
Research Fellow, Democracy & Resilience at GLOBSEC Bratislava

Laura Loguercio
Journalist at Pagella Politca / NTCenter

Andy Stoycheff
Director at NTCenter & Adam Smith College of Management

Caroline Schmidt
Security Policy Adviser at Austrian Federal Ministry of the Interior

Host

Ross King
Head of Competence Unit Data Science & Artificial Intelligence at AIT Austrian Institute of Technology

02.12.2020

UNDERMINING DEMOCRACY

Session Summary

Dominika Hajdu and Miroslava Sawiris, research fellows at the GLOBSEC Democracy & Resilience Programme, opened the programme with several alarming statistics. They cited an MIT study from 2018 showing that fake news disseminates faster than normal information. This may be because fake news targets strong emotions such as fear or hate.

They went on to cite results from their own surveys that show that nearly half of central and eastern European citizens do not believe in democracy, more than one-third believe that the COVID pandemic has been exaggerated by public authorities, and one-third believe that COVID-19 does not exist at all. They pointed out that the public health implications of these beliefs are grave, as this suggests that an insufficiently large segment of the population would be willing to be vaccinated, undermining the effectiveness of vaccination for the population as a whole.

They also noted that these beliefs are more likely to be found among disenfranchised, disadvantaged or otherwise vulnerable members of the population.

The GLOBSEC fellows then recommended a course of action in the form of cooperation between governments and NGOs:

- Build trust through strategic communication, cooperation and good planning
- Regulate social media
- Support quality journalism and they referred to positive international examples from Taiwan and New Zealand.

Caroline Schmidt, security policy adviser at the Austrian Ministry of the Interior, pointed out how citizens' social life has a strong online aspect, particularly during the pandemic, and that as a result, online platforms and applications dominate the content and flow of information online – while at the same time traditional media is losing ground. Social media applications use algorithms that form 'filter bubbles', in which the consumer only sees confirmation of existing beliefs. She also pointed out that this online ecosystem is vulnerable to hostile actors (from individuals to states) that can take advantage of recent advances in Artificial Intelligence (AI) to influence public discourse through, for example, deepfake videos or 'bot' swarms that can overwhelm Twitter streams.

Caroline noted several government activities, including an Austrian Disinformation Taskforce during elections, the KIRAS national project for disinformation detection defalsif-AI involving multiple government agencies, and also the EU Action Plan against Disinformation.

Laura Loguercio, a journalist currently working for the fact-checking website Pagella Politica (https://pagellapolitica.it/), reported on a joint investigation conducted with the NTCenter and de facto researcher Andy Stoycheff. The article, published on the website of The Social Observatory for Disinformation and Social Media Analysis (SOMA), explored how our cognitive layers contribute to the way we manage misinformation, and make us believe or deny the claims we hear on a daily basis.

Laura pointed out that fake news has played a prominent role in the ongoing COVID pandemic, not just in delegitimising important public health measures (such as wearing masks or respecting social distancing), but also in promoting scores of completely baseless miracle cures and remedies.

Laura also emphasised that the problem of fake news is borderless, and one important ongoing countermeasure is to build up collaborative platforms for journalists and fact checkers such as the SOMA Observatory (www.disinfobservatory.org) and the CoronavirusFacts Alliance (www.poynter.org/coronavirusfactsalliance/).

However, she also pointed out that there is an intrinsic limit to fact-checking: No matter how solid the evidence, or how clearly it is presented, fact-checking analysis will only be effective if the media consumer is open to receiving new information.

Andy Stoycheff, director of the NTCenter, presented his opening statement through a scenario involving the comic-book villain Brainiac, whose sidekick is empowered to observe the mental states of people around him. Through this story, which illustrates many aspects of his recent research, Andy pointed out that evolved mechanisms in the brain can pose cognitive stumbling blocks for every human being:

- Contexts that evoke fear can lead to sensory perceptions bypassing the pre-frontal cortex (the 'thinking' part of the brain) and going straight to the amygdala (the 'acting' part of the brain).

- Our brain automatically defends itself against information that conflicts with existing beliefs – the brain can actually condition the senses to ignore certain information.

- We cannot learn effectively from things we cannot directly observe (e.g., climate change).

Some of the panel's conclusions: Governments and NGOs must cooperate in order to address the borderless international challenge of disinformation.

Citizens need to be made aware of disinformation tactics and provided with tools to combat their own cognitive biases.

As in healthcare, when it comes to disinformation, prevention is more effective than reaction.

FAKE NEWS – The New Role of Media

Speakers

Katharina Schell
Member of the editorial board, digital innovation, media editor at APA – Austria Press Agency

Nikos Sarris
Head of Technologies Against Disinformation at the Athens Technology Center (ATC) Innovation Lab

Wolfgang Renner
Head of the Wiener Zeitung Academy at Wiener Zeitung

Host

Wolfgang Renner
Head of the Wiener Zeitung Academy at Wiener Zeitung

02.12.2020

THE NEW ROLE OF MEDIA
Session Summary

Moderated by Wolfgang Renner

Since 2007, Wolfgang Renner has headed the Academy of the Wiener Zeitung, the oldest daily newspaper in the world (1703) and owned by the Republic of Austria. He is responsible for relationship management with several stakeholders, for business collaborations with the publishing house, and for networking with partners in relevant socio-political fields.

He also has extensive experience in organising transnational, high-level discussions in the fields of science, culture and the economy. He was formerly Head of Corporate Communications at Austrian Research Centers and at Austria Today, which produces science and culture magazines in three different languages to raise Austria's profile in more than 170 countries.

In addition, he lectures at higher education institutions including the University of Applied Arts (Art & Economy), the Danube University (Interactive Media Center), the University of Vienna (Department of Communication) and the University of Applied Sciences BFI Vienna (Technical Sales Mangement).

Wolfgang Renner holds a Master of Science (MSc) in Communication and Management, studied Communication Science, Journalism and Philosophy at the Vienna University, and is an academically certified advertising and marketing manager. He is the first European to be awarded an honorary doctorate in communication sciences by the Academy of Journalism and Communication in Hanoi, Vietnam.

With his expertise in media literacy programmes for various target groups, he was predestined to moderate this ambitious panel.

To mark the discussion space for the panel with an expert in digital communications and a scientist, he opened the session by quoting the great American linguist, philosopher, cognitive scientist, historian, social critic and political activist Noam Chomsky from MIT:

"He who controls the media controls the minds of the public!"

Mr Renner reminded us that media is system relevant, and should be the fourth pillar of democracy, yet today we are living in times of the biggest loss in confidence and trust in the media since its founding.

He set the framework for the discussion with the panellists by posing the following questions:

How do you deal with alternative facts, false narratives or conspiracy theories in your daily routines as a journalist (fact-checking) or scientist (research)?

Is social media still a sign of hope for a free world (freedom of expression) and how has social media changed our societies (hate speech)?

Why do we believe in fake news? – A journey into the cognitive layers of disinformation.

Mr Renner cited the renowned London School of Economics which defined "5 Giant Evils" in its 2019 report "Tackling the Information Crisis" to question the consequences of media change on the overall system:

- Confusion about what is true, and whom to believe
- Cynicism, losing trust in trustworthy sources
- Fragmentation into parallel realities, truth publics
- Irresponsibility by organisations that lack a developed ethical code of responsibility
- Apathy, citizens are losing faith in democracy

He then asked the panellists how social media is influencing its users, especially young people, and what can be done to safeguard our democracies against mass manipulation and disinformation.

In a closing round, Mr Renner asked about the biggest challenge the global media industry is facing today. He is very well aware that cuts in media budgets everywhere only heighten the problem, making it even harder to come up with effective solutions. In his opinion, it has never been more important to apply the journalistic imperative of check, double-check and re-check in verifying any news in order to reconquer trust in traditional media amongst wider audiences.

<u>Katharina Schell</u>
As managing editor at the Austria Presse Agency (APA) Ms Schell oversees digital innovation projects for the newsroom as well as for the agency's markets. Over the course of her career as an editor, she has been witness to the digital transformation and its impact on the profession for more than 20 years; journalism has become technology driven, but she prefers to regard this as an opportunity rather than a threat. APA has been tackling the digital challenges for years now, and is focusing on topics such as fake news, data-driven

storytelling and workflow automation. Recent projects in the newsroom include automated journalism, a new verification unit and a major overhaul of the distribution platform.

The uniqueness of journalistic storytelling is a human strength and I do not see any substitute soon. We will definitely need experienced journalists for more than a couple of years to produce trustworthy news.

In a period of declining trust in the media and the massive spread of fake news, transparency has become a key criterion in journalistic practice. We always have to ask ourselves where the initial information came from. From a broader strategic perspective on disinformation, we have to adapt our journalistic tools to be able to verify and prove news sources and their disseminated content. At APA, we run a special verification unit and have installed a verification officer to succeed in this difficult task. The unit consists of editors and journalists with an additional specific skillset to verify news. Today, counteracting fake news is a major challenge for every newsroom. It is very alarming when journalists of traditional, legacy, old school media are denounced as liars in social media. Terms like Lügenpresse are used to claim that print media are no longer telling the truth. We have to prove that this is wrong.

Publishers have to deal with new emerging channels and platforms, as well as a major shift in media consumption habits. Social media users often argue that if news is important enough, it will find its way to them ("news will find me"). Users then pass this information on within their communities and peer groups. This is primarily regarded as a phenomenon in younger age groups, but I would like to point out that there have been several studies showing that young people are consuming news in a very critical way.

'Robot journalism' is currently overrated hype. No machine is able to gather unstructured data and tell a plausible, truthful story. Successful examples of automated journalism use Natural Language Generation in order to anticipate future data and stories. But this is actually a fairly new dimension of data journalism, and there are no robots whatsoever involved. There is doubtless a huge potential for automation in newsroom and amongst journalists. This also implies the need for additional digital skills, know-how and tools, and a better understanding of data structures.

Nikos Sarris

As a senior researcher at ITI/CERTH (Information Technologies Institute) and Head of Technologies Against Disinformation at ATC (Athens Technology Center) in Greece, and coordinator of the SOMA (Social Observatory for Disinformation and Social Media Analysis) project and EB member of the EDMO (European Digital Media Observatory) project, for many years the focus of Mr Nikos Sarris' scientific work has been understanding news content and assessing trustworthiness. He was therefore the perfect session counterpart to Katharina Schell, who reflected on the new role of media based on her insights into the daily routines at a national news agency.

The decay of trust towards the media is one of the greatest problems our societies are facing today. As a sector, the media has allowed this to happen by failing to protect its reputation with high quality, responsible journalism of a sufficiently large scale. This has allowed actors with questionable intentions to penetrate the media scene and corrupt the image of journalism to an unprecedented degree. To undo this harm, professionals and organisations operating in responsible journalism must consistently work hard to reclaim their lost reputation. This can only be achieved through high quality journalism, in which any claim is supported by well-established facts and proof beyond reasonable doubt. This is not easy, and collaboration between determined actors will be necessary. Support from official institutions will also be needed to organise collaborative work, while maintaining the integrity and transparency of such efforts. The SOMA and EDMO projects are engaged in this endeavour, building collaborative communities to monitor and report on disinformation campaigns. More than 80 organisations have joined the European Observatory Against Disinformation operated by SOMA, soon to be transitioned to EDMO.

Social media have played a major role in quickly spreading news to every corner of the world. Unfortunately, this medium has been more actively exploited by malicious actors to propagate false information. By taking advantage of cognitive biases deeply rooted in our brains, they can quickly and easily mislead us. This does not mean that social media should be condemned, however, the relevant actors must team up to limit this ever-growing plague of disinformation, by uncovering malicious intent and educating the public on how to resist to such practices and protect their free way of thinking. Recent research by our colleagues in the SOMA network discussed key aspects of cognitive biases that affect our comprehension of misinformation: we tend to believe narratives which are close to our existing beliefs; we often live in 'filter bubbles', tending to follow people who express opinions that conform to our beliefs; and we tend to believe information that we have come across repeatedly.

Some of the panel's conclusions:

Wolfgang Renner:
"The highest value is trust"

Katharina Schell:
"Transparency is the key for trust in news"

Nikos Sarris:
"Collaboration against disinformation is a must"

Wolfgang Renner

AUSTRIA IN SECURITY RESEARCH - THE DIGITAL DIMENSION


© BMLRT

Keynote

Andreas Reichhardt

Vice-Minister at the Federal Ministry of Agriculture, Regions and Tourism, on behalf of Federal Minister Elisabeth Köstinger

Dear Ladies and Gentlemen,

I feel most honoured to be part of the opening slot at this timely high-level event. Let me begin by expressing the best wishes on behalf of my Minister, Ms Elisabeth Köstinger. Being in charge of the Austrian security research programme KIRAS, the national defence research programme FORTE and the roll-out for broadband networks in Austria, she regards international conferences like today's IDSF as important tools to foster cyber security.

I would like to use the next few minutes to underline the importance of research, especially in the field of cyber security, and sketch out the principles Austria has chosen to address this matter. Security is the very foundation of every successful and lasting society. Its existence is a basic need for its citizens and its fulfilment the noblest task for every government. However, like society itself, security challenges are ever evolving. Who would have thought a year ago that the greatest accelerator as well as threat to our digital transformation would be an organic virus?

Still, it was COVID-19 which created two imminent dilemmas for cyber security:

- The 'structural dilemma' of digital transformation: The more all ways of life are transformed by cyber, the stronger the underlying infrastructure needs to be and the more urgent the need to protect necessary critical infrastructures like broadband and energy networks becomes. This leads to
- the 'application dilemma' of digital transformation: The stronger the underlying cyber infrastructure becomes, the more applications will be invented to use this infrastructure, and the more urgent the need to protect users against cyber security challenges like cyber attacks, cyber crime, fake news and propaganda becomes.

These two dilemmas reinforce each other and can quickly lead to a dangerous cycle. The solution to these dilemmas is twofold:

- On the one hand, cooperation and exchange beyond borders and between all stakeholders is vital to assess what is happening in cyber security today. This conference, the International Digital Security Forum, is a perfect example of how to do this right.

- On the other hand, applied security research is vital to provide the tools and answers to what will happen in cyber security tomorrow.

Austrian security research acknowledged early on the need for a sober and open approach towards the topic, and acted accordingly. Ditching the classic scenario of military-led territorial defence, a new, much broader security notion with a civil focus emerged, encompassing non-military challenges such as the fight against terrorism and organised crime, the management of natural disasters, and, of ever-growing importance, cyber security.

The KIRAS programme architecture is set up to deal with all relevant questions regarding security, economic and social policies in equal measure. Any successful KIRAS project must mandatorily include:

- Public end users, to guarantee that only projects providing practical solutions are funded;

- Austrian companies to transform successful research results into products and services and into future creation of value in Austria;

- Experts on the Humanities, Social Sciences and Cultural Studies as guardians, to find technological solutions which truly contribute to greater security and support the development of alternative, non-technological solutions to security questions; and naturally

- Researchers to make the necessary innovation happen.

From its start in 2005 to this day, KIRAS calls have received a budget of € 103 million to successfully fund 300 projects. Many of these projects deal with a wide array of cyber security topics. Some tackle cyber forensics for virtual currencies, automatic anomaly detection in digital control systems, and security for smartphone app users. Others address the complex problems of online hate speech and cyber bullying, or the defence against Advanced Persistent Threats.

In 2018, to complete the comprehensive approach taken by Austrian security research, and as a response to growing awareness of cyber defence, my Ministry, in close cooperation with the Ministry of Defence, created Austria's first national defence research programme, FORTE.

Our experiences so far lead to the conclusion that any action related to cyber security must be driven by the involvement of all relevant actors. Therefore, I am proud to see so many of the experts on today's and tomorrow's panels are also active in KIRAS and FORTE. Furthermore, any successful cyber security measure needs societal endorsement, because only if citizens feel more secure, will there be more security. The current heated debates in Europe on privacy rights and end-to-end encryption are a lively reminder of this.

When it began, our digital age was heralded as an important step in achieving freedom from fear. Let us make sure that it does not become a threat in itself. Thank you all, dear participants, for your efforts in this important endeavour and congratulations to the organisers at AIT and the Austrian Federal Economic Chamber for setting up such an impactful event.

AN AFRICAN PERSPECTIVE ON DIGITALIZATION

Keynote

Speaker

Hon. Vincent Waiswa Bagiire
The Permanent Secretary at Ministry of Information Communications Technology and National Guidance

Moderator

Philipp Agathonos
Diplomat, Civilian Crisis Management, CSDP Training, Peace & Security at Federal Ministry for European and International Affairs

Uganda has been a priority country for the Austrian Development Cooperation since 1992. With its Digital Transformation Programme, it aims to increase ICT penetration and the use of ICT services for social and economic development, thus making a major contribution to the National Development Programme.

The Hon. Vincent Waiswa Bagiire, Permanent Secretary at the Ministry of Information and Communications Technology and National Guidance of Uganda, presented his country's Digital Transformation Programme at the IDSF. The Programme pursues five objectives:

1. Increase the national ICT infrastructure coverage;
2. Enhance use of ICT in national development and service delivery;
3. Promote ICT research, innovation and commercialization of indigenous knowledge products;
4. Increase the ICT human resource capital;
5. Strengthen the policy, legal and regulatory framework.

During the discussion moderated by Philipp Agathonos (MFA Austria), he talked about his approach to digitalisation and security in Africa, and the opportunities his country offers for research, innovation and business actors in Europe, and in particular in Austria.

DIGITAL RESILIENCE & COMPLEXITY

Summary

Introduction

"Resilience is the capacity of a system, enterprise or person, to maintain its core purpose and integrity in the face of dramatically changing circumstances.", Andrew Zolli

Information and Communication Technology (ICT) is the digital nervous system of our society and plays a decisive role in making our society resilient or fragile. ICT influences and connects all sorts of technologies, and forms extremely complex systems of systems which are increasingly hard to control, understand and change.

In this session we focused on a web of aspects that influence each other in interesting and also potentially dangerous ways: innovation (talk) and progress; complexity of systems and maintenance:

Innovation as such is only a small cog in the large machinery of progress — just as evolution cannot be explained by mutation alone. Other parts of this 'machinery' are selection and cooperation, public discourse and a generalist mindset that allows us to connect the dots between the many details we find in research today. An innovation cannot be progress if it makes society vulnerable and fragile — particularly considering the threats of our time, from climate crisis to our failing economic systems. Hence risk management and precautionary measures are essential, but also very challenging in such complex environments.

If nothing else, maintenance deserves special consideration. To quote the late David Graeber: "Most work is keeping things the same: you buy a cup once but wash it a thousand times." It is easy to forget that maintenance is the foundation of a resilient society. Moreover, maintenance and sustainability are just two sides of the same coin. There is also a striking relation between maintenance and innovation: successful innovation translates to infrastructure that needs to be maintained on top of, and connected with, all other infrastructure we already have in place. Is this sufficiently considered in the design, selection and budgeting process? Or do we just aim for the new?

Unleashed complexity makes progress harder and harder over time. We lose control, side effects become unmanageable, our infrastructure fragile. ICT plays a pivotal role as a moderator or amplifier of complexity — depending on our architectural and management skills.

Alexander Schatten discussed these topics from two angles — brackets — if you will: on the one hand, with Dr Andreas Windisch: How can we handle complexity? What can we learn from physics and how do we educate our young people? And on the other, with Dr Lukas Feiler: innovation needs structure and complexity crash barriers that are strong yet flexible. Is our legal system capable of structuring a resilient society that needs to handle uncertainty?

Lost in Complexity: Digital Escape – or Resilient Future?
Andreas Windisch

Physics has demonstrated amazing achievements over the last 150 years. Achievements, that were not just innovations, but also led to actual social progress. We are able to describe and predict a number of physical systems with astonishing precision.

Today digitisation, big data and artificial intelligence (whatever that means exactly) promise a detailed understanding of our world and the people in it (at least in popular interpretations). How close are we to precisely predicting our economy, people's behaviour, the climate crisis? Will decisions just be a logical consequence derived from data? Forget politics, just follow the science?

Or do we instead face fundamental limits of prediction and knowledge in complex systems? Can we get lost in the game? And, by the by, who decides the rules of the game we are playing? Can incentive systems be improved from within, or is Kurt Gödel still correct 90 years later?

It seems making decisions under uncertainty is something quite different from evidence-based decision making.

So finally: what does that mean for education, science, universities? Do we need more generalists/all-rounders and fewer experts who get caught up in ever smaller details? Are we teaching pupils and students the right skills to understand this difference? Do we really need more digitisation in the classroom? Is today's university capable of working on progress or do universities themselves fall into the trap of innovation talk?

Resilience, complexity and good maintenance the legal aspects
Lukas Feiler

The legal system should be a foundation for progress and play an important role in defining a scaffold for resilient societies. However, complex and resilient systems have no clear targets, goals and descriptions, not even clear responsibilities. Do we have to live with ambiguity, and unclear and unpredictable effects of technology, or can we regulate every detail of our society? Our current legal system seems to struggle with that question.

To paint a bigger picture: what are current drivers of legislation? Do we see too much politicking? Where is political small change generated: in announcing new legislation or in its tedious execution?

How much 'precision' is desired in our legal frameworks? It appears that in complex settings inflexible and over-detailed regulation tends to fail or create unintended consequences. Complexity is not only the enemy of technology but also of legislation. The conjecture is: complexity cannot be tamed by complex legislation. Complex legislation tends to worsen the problems it intends to solve.

Resilience requires diversity and agility — is the legal system fit for that challenge? What can we do to improve the situation?

Besides, do technical systems (and ICT systems in particular) exhibit special characteristics and challenges for the legal system? For instance in some cases, such as encryption, we seem to face 'tipping points', in the sense that when certain lines are crossed the whole building metaphorically collapses.

Is the public discourse immature? It appears that 'nerds' lack agility when their pet technology is under scrutiny while, more often than not, legal systems seem unwilling to accept ambiguity and shades of grey.

On top of that, we are in a situation in which major technological transformations are driven by just a few monopoly players who seem too big to manage. Even the USA or EU appear too feeble to stand up to the legal challenges. How should we handle this difficult interplay between technology, law and economic systems?

Speakers

Alexander Schatten
Senior Researcher at SBA Research

Lukas Feiler
Partner at Baker & McKenzie Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Andreas Windisch
Theoretical Physicist, AI specialist at Know-Center

Host

Alexander Schatten
Senior Researcher at SBA Research

As a follow up for German audiences listen to
- Zukunft Denken Episode 18: Gespräch mit Andreas Windisch: Physik, Fortschritt oder Stagnation www.podcast.zukunft-denken.eu/e/018-–-gesprach-mit-andreas-windisch-physik-fortschritt-oder-stagnation/
- Zukunft Denken Episode 35: Innovation oder: Alle Existenz ist Wartung? www.podcast.zukunft-denken.eu/e/035-wartung/
- Zukunft Denken: Gespräch mit Lukas Feiler – stay tuned!

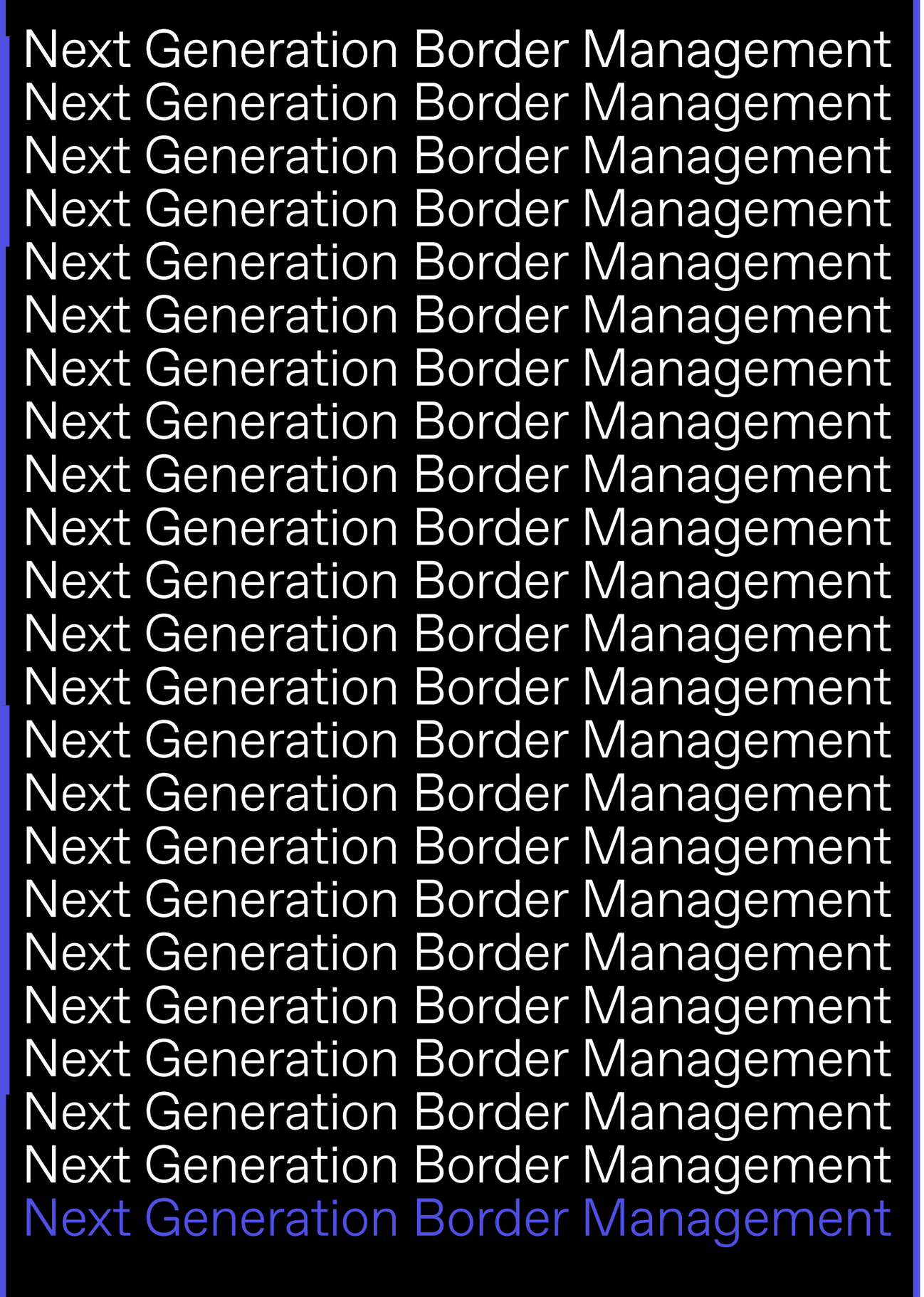
Opinion piece (Alexander Schatten):
- The long shadow of innovation, or: Lean Digitisation and the Car: https://sichten.blogspot.com/2020/11/the-long-shadow-of-innovation-or-lean.html

Alexander Schatten, Lukas Feiler

Andreas Windisch

“Resilience is the capacity of a system, enterprise or person, to maintain its core purpose and integrity in the face of dramatically changing circumstances.”

Andrew Zolli



Speakers

Giulio M. Mancini
Policy Officer at the European Commission – DG Migration and Home Affairs

Romain Nivelle
Director at Mission to the EU of the Hauts-de-France Region

Georgios Boultadakis
Deputy R&D Director at European Dynamics Luxembourg SA

Pantelis Michalis
EU Projects Coordinator at the Center for Security Studies (KEMEA)

James Ferryman
Professor at the University of Reading

Host

Andreas Kriechbaum-Zabini
Thematic Coordinator at the AIT Austrian Institute of Technology

The NEXT GENERATION BORDER MANAGEMENT panel session gathered together experts representing all relevant stakeholders in the field: practitioners, academia and research, industry and policy makers.

Efficient border management is essential for maintaining a fully functioning Schengen area and the enormous achievement of free movement within it. We are currently experiencing how threats such as the current pandemic or the migration crisis might affect free movement.
The panel discussed how the joint efforts of all stakeholders in research and innovation can usher in the next generation of border management, and addressed the needs to set common requirements, to find a trade-off between security and facilitation of movement for persons, goods and services, and, finally, to present the research results to practitioners and improve exploitation.
The panel was hosted by Andreas Kriechbaum-Zabini, Thematic Coordinator at AIT, who has focused on research and innovation in the field of border management for 10 years, contributing to national and international projects – also in the role as coordinator – in the field of surveillance and protection.

The panel experts are:
Romain Nivelle, Director at the Mission to the EU of the Hauts-de-France Region (France), a post he has held since the Hauts-de-France Region was founded in 2016. He specialises in the interactions between the regional dimension and the European Union, with particular reference to economics and social issues.

Pantelis Michalis, EU Projects Coordinator at the Center for Security Studies (KEMEA), Greece. During his military career, he was a Commander, Project Officer and Staff member in positions of responsibility within the Hellenic Armed Forces and the Ministry of Defence, encompassing military communications, border surveillance, mapping, intelligence, defence and space policy. Since 2018 he has been project coordinator at the Center for Security Studies (KEMEA) of the Hellenic Ministry of Citizen Protection, and he is involved in national and EU-funded projects related to border surveillance and the fight against crime and terrorism.

James Ferryman, a professor at the University of Reading, is a computer scientist and leads the Computational Vision Group within the Department of Computer Science, School of Mathematical, Physical and Computational Sciences (SMPCS), University of Reading. His current research interests include multimodal biometrics, automated video surveillance and benchmarking (performance evaluation). He has participated in a wide range of UK and EU-funded research projects in the security field.

Georgios Boultadakis, Deputy R&D Director at European Dynamics Luxembourg SA. For 15 years, he worked as an engineering manager with the Hellenic Air Force, as well as a quality control/assurance engineer. He joined European Dynamics in 2014 as a Senior R&D consultant, where he has participated in and coordinated research projects in the fields of security, cyber security, energy and smart manufacturing for European Commission-funded research programmes. His research interests include future ICT, signal processing, pattern recognition techniques and electromagnetism.

Giulio M. Mancini, Policy Officer at the European Commission – DG Migration and Home Affairs. He coordinates EU border and external security innovation policy in the Innovation and Industry for Security Unit of the Directorate-General for Migration and Home Affairs of the European Commission. He was previously project officer on security research and programme manager for the Union actions of the Asylum, Migration and Integration Fund of the European Union.

In the discussion the panellists addressed the following questions:

- Can Europe's borders be both open, to allow for the cross-border flow of legitimate trade and commerce, and secure, in the sense that the national security interests of states are protected?

- How do the European Commission, national authorities, major industries and research organisations commit themselves to achieve a balance between the need to maintain security against cross-border threats and the freedom of movement for persons, goods, services and capital?

- How can border guard authorities be supported in achieving acceptable European border management which strengthens cross-border cooperation and border surveillance in a counter-terrorism context?

Romain Nivelle shared his views and experiences as a practitioner about integrating the results of European innovation research into operative systems at the regional level. In an effort to anticipate the possible consequences of the Brexit agreement, the Hauts-de-France region implemented a pilot project to enhance security and fluidity at the maritime border after Brexit. The region is not directly responsible for border management, but the UK decision will have a strong impact as the region has a strong maritime border at the heart of the Channel. Furthermore, the region owns the port of Calais which is directly connected to the port of Dover in the UK, and sees the transit of about 10,000 lorries per day. The region's pro-active strategy has been to negotiate

a public procurement process in order to experiment with innovative technologies for a fluid and secure border, developed in the FP7 EU-funded project FASTPASS, led by AIT, and involving partners such as Veridos and Magnetics.

The FASTPASS project developed innovative automated border control systems (e-Gates) that include a 'drive through' concept for passenger cars and lorries. The solution was tested under realistic conditions in summer 2019, with the involvement of all stakeholders and end users (French and UK border forces, prefectures, ferries and harbour operators, regional council etc.).

The FASTPASS lane enables the following automated checks: passport scanning, chip reading, passport verification, biometric face verification, and database checks with each national authority. Results are displayed to the border guards for the final decision. The evaluation of the system brought very promising results in terms of security, fluidity and use of human resources. The average duration of the checks is 48 seconds per car, and checks of up to four people can be done simultaneously. This enables single border guards to supervise multiple e-Gates. Furthermore, the solution enables a joint control process in which relevant data are delivered separately to the UK and the French border guards, so that no interaction is needed between the databases of the different authorities.

Pantelis Michalis brought to the discussion the perspective of an additional relevant practitioner, the Center for Security Studies (KEMEA), which operates as a think tank for innovation and technology in the field of national security policies for the Hellenic Ministry of Citizen Protection. KEMEA research activities cover a very large portfolio of projects in the security context. Projects in border external security account for 14% of the centre's activities. KEMEA works in close cooperation with the Hellenic police and coastguards on research and development projects to set up common demonstrations, trials and evaluation of best practices and operational solutions. Further focuses of activity are know-how transfer, studies of national security and upgrading equipment, resources and facilities. Two research projects that exemplify KEMEA's approach to addressing the questions posed above are Andromeda, funded under the EU H2020 programme, and EWISA, which was funded under the EU-FP7 programme and was concluded in July 2019. Andromeda's aim is to demonstrate applied solutions which enhance border and external security. One of the most important goals is to enhance the established CISE data model for maritime surveillance to include land surveillance (e-CISE). Test and validation are essential to the project: 8 months of testing in a real operational environment, including training, have been accomplished. The project results were demonstrated to Frontex Executive Director Mr Leggeri and the Hellenic Minister of Citizen Protection in the Evros border area in July 2020.

The EWISA project was coordinated by KEMEA and, for the first time in an EU-funded project, involved the participation of four authorities from EU Ministries of the Interior that jointly determined their vision for surveillance of the external EU borders within the EUROSUR framework, the EWISA common concept and the validation strategy under the innovation procurement scheme. The testing phase in EWISA was again very extended, which is essential for solid, validated conclusions. Tests were performed in four different geographical areas over a period of 8 months, with border guards using the system in their routine operations.

The lesson learned from EWISA, which can be applied more broadly, is that the public sector can drive innovation. Effective cooperation was achieved among the border authorities, with public research agencies taking a critical role. Furthermore, the link between end users and industry extends the benefit of innovation procurement. The involvement of EU agencies, especially Frontex, is very important and is also desirable in the future. EU funding in innovation procurement is definitely needed.

KEMEA is strategically involved in PCP projects and probably PPI in the future, and is currently leading all PCP projects in the security sector.

James Ferryman from the University of Reading pointed out the relevant issues in future border management from the academic research perspective. It is a matter of fact that there is increasing pressure on border authorities to enable travel across countries, while maintaining – if not increasing – security. To achieve this requires new mobility concepts that use advanced technologies to increase the accuracy and improve the efficiency of border checks, while simultaneously being cost effective through better resource management. Speeding up crossing times for travellers is to be achieved by enhancing traveller guidance, performing extensive processing in advance, and efficiently indicating to border guards the travellers who must be checked further.
Research organisations address these challenges by investing in research and development of new mobility concepts. James' research group places a particular focus on data science to implement the above mentioned new mobility concepts, exploiting both biometrics in an enhanced way as well as related technologies such as mobile devices. Advance risk assessment is also a highly relevant aspect.
A good case study in this respect is the EU's H2020 three-year project PROTECT (www.projectprotect.eu), coordinated by James, to explore the use of advance contactless biometrics at the border.
The project focused on increasing the number of biometric modalities with counter spoofing to enhance security.
The project also examined technologies including digital travel credentials which use the traveller's own smartphone, and next generation ePassports (advanced passports). The identification process was split into two stages: enrolment prior to the border crossing; and verification on the move using biometric identification of the traveller at the border. Finally, user centricity and privacy was also a pertinent aspect of PROTECT. The use of the developed smartphone app allows travellers to maintain visibility and control over their biometric and biographic data. A very comprehensive ethical and legal assessment was undertaken to achieve the objective of enhanced privacy and data protection.

Future research must clearly support border guards applying more advance data science methods such as multimodal biometrics on the move, and especially wider and more extensive traveller risk assessment. A broad set of technologies and systems will be needed to achieve this, including information systems that perform early checks at, or before, crossing the border. The ideal is a no-gate crossing solution, supported by a wider risk assessment check that considers the whole identity lifecycle. A follow-on project D4fly (www.d4fly.eu) is examining some of these issues.

George Boultadakis' contribution focused on the approach taken by a large company like European Dynamics (ED) which is specialised in ICT services. The private sector also shows strong interest in participating in R&D projects in order to generate knowledge about the real challenges in the European context, to be involved in developing innovative concepts and technologies and using advanced technologies and frameworks, and to gain a very thorough understanding of the balance needed between advanced security, enhanced user experience, technological innovation and ethics. ED is a leading ICT services provider and software developer. As such, it has a significant portfolio of security products and services and customers such as governmental bodies, European institutions and international organisations all over the world. The main objective of its activities in the security field – addressed via a large portfolio of projects, both commercial and research-based – are to support increased traveller flows and international trade, to improve the quality of the user experience, to address interoperability and standardisation issues, to address the needs of the European framework for security, and to advance the role of ICT as an integral part of the solution.

The challenges with which ED has to cope are, first of all, limited system interoperability – currently information is not shared across agencies and among the different stakeholders. Furthermore, there is an exclusive case-by-case approach. Finally, the time to market for research outcomes is very long, in certain cases because of regulatory constraints, as well as hesitancy among vendors to invest. The way to address these challenges is first by establishing a common approach among stakeholders in order to move towards collaborative border management. At the same time, consistency must be ensured by having well-established processes and standards to enable interoperability among stakeholders. There is also a need to increase the contribution made by novel technologies, and this should be embedded in an agile approach to introduce dynamic and flexible systems for intelligence-driven risk management, simultaneously encouraging support for cutting-edge technologies to achieve high levels of control and facilitation.

Giulio M. Mancini provided the perspective of a representative of the European Commission, which is funding many of the projects mentioned in the discussion. The Directorate-General for Migration and Home Affairs (DG Home) manages the part of the EU research framework programme covering civilian security research. Innovation and technology are prominently acknowledged within the EU security policy. In recent and past EU internal security strategies, the transformation capacity of innovation and technology is recognised, as well as its potential to recognise and address future challenges. It is also recognised in the new Pact for Migration and Asylum, especially for integrated border management to protect the Schengen area, and to strengthen the capacity for maritime search and rescue.
It is also well addressed in the EU Customs Union's action plan for customs and supply chain security.

The security research programme within H2020 is one of the instruments to invest in innovation and technology for civil security. Civil security research has been in place since FP7, continues in H2020, and will be part of the upcoming Horizon Europe programme over the next 7 years. Since 2007, around 700 research projects have been funded at a cost of over EUR 3 billion. These have been very large, multi-stakeholder and transnational research efforts. If we consider that only a few European Member States have national civil security research programmes, the contribution made to civil security by European funding is even more substantial.

Moreover, it is important to have a European approach to security innovation both for reasons of strategic autonomy, and because European innovation goes hand-in-hand with aspects including privacy by design, data protection principles, respect for civil liberties and fundamental rights.

In the thematic area of border security within the H2020 framework programme, 31 projects have been funded with a volume of more than EUR 140 billion since 2014, and five more projects will be funded in the last call for another EUR 40 million this year. Funded research includes border surveillance, future border control technologies, ethical, legal and societal impact assessments, security and supply chain and customs for the flow of goods, as well as external civilian security.

The uptake challenge always follows research. The market for civil security is a small and closed group of buyers. Furthermore, it is a fragmented market in Europe, traditionally coming from national systems. Innovation must necessarily address the practitioners, and the Commission is making efforts in this direction, such as inserting research and innovation investments into a broader, capability-based long-term approach. This approach includes actively involving practitioners in the research process, funding networks of practitioners to discuss innovation, launching initiatives such as the community of users for safe, secure and resilient societies and the annual security research event, using procurement of innovation (or 'pre-commercial procurement') and finally building more synergies with other funds to enable deployment, test validation etc., and ease the transfer into operation.

Finally, a particularly important collaboration is that with Frontex,for its role to assist Member States in building European capability development plan for border management, and to assist the Commission in ensuring that the EU border security research programme is made available to practitioners. An agreement on this was signed this year.

Take home messages

The panel identified the take up of technological innovation as one of the major priorities to be addressed in the future. There is a need to strengthen mechanisms and wide-ranging processes to embed research so that it can be exploited by practitioners.

Further future challenges include interoperability and scalability. The regulatory processes are already in place and the technology is mature. What is now needed are mechanisms to put the collective knowledge under one umbrella, and target an open solution able to accommodate different technologies and solutions, and make them available. There is thus a need to:

- Establish a common understanding and promote the effective integration and cooperation of authorities and all stakeholders in the value chain. The move towards collaborative border management should be intensified to overcome critical issues such as resource management, the costs of systems procurement, etc.

- Introduce consistency in processes, to foster certainty and trust for travellers and traders and empower border authorities through well-established concepts and precise standards.

- Increase the contribution of innovative technology to international passenger flows and trade as a key enabler for border management reform.

- Establish agile means of operation because demands will become even greater and more diverse as the years pass; it is now more necessary than ever to introduce dynamic and flexible systems for intelligence-driven risk management.

Advanced Biometrics for Counter Terrorism

Speakers

Nelson Goncalves
Senior IBM Specialist – Manager of the IOM African Capacity Building Centre at IOM – International Organisation for Migration

Reinhard Schmid
Head of Central Identification Services at the Austrian Federal Ministry of the Interior

Andreas Wolf
Principal Scientist Biometrics at Bundesdruckerei GmbH

Rocco Messina
Project Officer at the United Nations Counter -Terrorism Centre (UNCCT), New York, USA

Margherita Natali
Project Officer at the United Nations Counter-Terrorism Centre (UNCCT), New York, USA

Host

Bernhard Strobl
Thematic Coordinator at the AIT Austrian Institute of Technology

While there are recognised challenges in verifying biometric data and identifying individuals, the COVID-19 pandemic has created even greater obstacles for effective and safe data collection. These challenges include the requirement for individuals to wear masks, often making standoff collection of data more challenging, and concerns with respect to the safety of touch-based systems for biometric data collection. There is a need to expand the capabilities of biometric data collection and associated information sharing, and to explore touchless methods that support accurate and efficient collection and processing of data.

The goal of this session was to talk about possible new applications that can help us reduce physical contact with scanning devices while, at the same time, increasing security and convenience. We invited a panel of internationally renowned experts in this field and asked them for brief input statements that were then followed by a panel discussion, which also involved questions from the audience.

Reinhard Schmid, who is Head of Central Identification Services at the Austrian Federal Ministry of the Interior, was the first speaker on this panel. He presented a 3-minute animation about a typical identification problem within the EU: a non-Schengen visitor, changing identities across Member States, and hard to track because of a lack of interoperability. With new Article 20 IO Interoperability Regulations and the output of a pioneering research project – BioCapture – new possibilities are available: if used in real time, every policeman can use their smartphone to capture a minimum of eight fingerprints of a person on a street for identification purposes: hygienic, fast, with no additional effort and hardware requirements.

Next, Rocco Messina (supported by Margherita Natali) both Project Officers at the United Nations Counter-Terrorism Centre (UNCCT), New York, USA, talked about the responsible use and sharing of biometric data in the counter-terrorism context. The UNSCR 2396 (2017) states that: “1) Decides that Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law. 2) Encourages Member States to share this data responsibly among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies. 3) Calls upon other Member States, international, regional, and sub-regional entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems.” A human rights-compliant approach to biometrics is not possible without safeguarding the right to privacy and recognised data protection principles. A human rights-minded approach should govern all phases of design, development and deployment of biometric tools = “human rights by design”.

Andreas Wolf is one of the German DIN experts delegated to the ISO/IEC JTC 1 committees SC 17, SC 27, SC 31 and SC 37 (EU Committee CEN/TC 224). For him, the three essentials for applications dealing with biometric data are: interoperability, authenticity, and quality. Therefore, revisit best practice recommendations from time to time, make use of standards wherever possible, and consider backwards compatibility, in particular in large-scale applications. Privacy by design saves time and money. Asked about expected trends in biometric technology his answer was: we will notice an increase in touchless sensors (everywhere). Ease of use matters not only with respect to quality, devices must also be user-friendly. Security aspects get increased attention: PAD, morphing, etc. There is room to improve with face recognition, with higher quality and more comprehensive data of the face region (keyword: e.g., periocular). We also expect many more modalities and fusion of different data, including context data.

Finally, we had Nelson Goncalves, Senior IBM Specialist – Manager of the IOM African Capacity Building Centre at IOM – International Organisation for Migration. He gave us insight into legitimate concerns resulting from the use of new technologies. His answer to the question of whether biometrics will bring a better future was ‘yes’, as legal proof of identity, and as a means of combatting identity theft, all eventually backed up by additional blockchain technology. However, the correct legal framework must be followed: human rights. One way to go in the future is also to make use of trusted programmes for identity management and biometrics. One very impressive sentence was: acceptance comes from trust and trust comes from standardisation. He also stated that seamless/touchless solutions will arrive on the scene in the coming years – not just during a pandemic.

“WOMEN IN CYBER SECURITY”, ORGANISED BY THE WORLD INSTITUTE FOR NUCLEAR SECURITY
WEBINAR

Speakers

Chris Ensor
Deputy Director for Cyber Skills and Growth of the National Cyber Security Centre (NCSC) in the United Kingdom

Zoe Edmeades
Managing Director and Co-owner of The Security Company Limited

Sayako Quinlan
Digital Forensics Consultant and Co-Chair of the Cyber Security & Emerging Technologies Working Group at Women of Color Advancing Peace, Security & Conflict Transformation (WCAPS)

The World Institute for Nuclear Security (WINS) is committed to advancing gender parity in the hiring, retention, and promotion of women in nuclear security, especially in areas where women are significantly underrepresented. To this end, WINS conducted a webinar in the margins of the International Digital Security Forum, to identify best practices and ways forward to advance and amplify the role of women in cybersecurity.

Three leading voices in the field discussed the importance of a diverse and inclusive workforce, barriers to entry, opportunities, lessons learned & the way forward. In particular, they demonstrated how national organisations are advocating and championing girls in STEM subjects, how businesses are adapting and applying behaviour and cultural best practice, and how NGOs are advancing and amplifying the voice of women of colour in peace, security, and conflict transformation. Speakers discussed ways in which girls and women can be better educated/prepared/informed for careers in cyber security. They offered insights into pathways for success, yet cautioned that that there are obstacles to overcome, including corporate culture, lack of institutional support and access, and misperceptions about women and minority communities. It was clear that diversity is more than just a question of gender, and should also include considerations of race, socio-economic, and educational background.

A survey was distributed in advance of the webinar that was intended to objectively put the issue into context, and to identify actionable ways forward in addressing the under-representation of women in cyber security. The majority of respondents thought that women are significantly underrepresented in cyber security roles, which is perceived as a predominantly male profession. The main obstacle was identified as lack of information about careers in cyber security. The best method of increasing female representation in cyber was through targeted recruitment and training. Webinar participants concluded that this is in part because hiring campaigns pre-suppose that there are already qualified women or enough of them, when the opposite is true. The cybersecurity sector needs access to the entire workforce, not just half of it.

Keynote

NEW RULES FOR ECONOMIC AND CYBER SECURITY

Speaker

Mika Lauhde
Vice-President, Cyber Security & Privacy, Global PACD at Huawei Technologies Co., LTD

Often, especially in Europe, fear and sanctions are used to sell cyber security. It should not be this way. The motivation behind telecommunications has always been economic benefits and advancing human communication. Every generation in the telecom era has brought new cyber challenges, each addressed by new cyber countermeasures. And every time, the benefits have then led to potential negative issues.

But at the moment we are taking a deliberate leap. Not because of telecoms themselves, but because of the global recession caused by the pandemic.

So how, and where, should the world seek fast recovery, when at the same time Europe seems to be paralysed by the fear of potential cyber issues associated with future innovations?

It currently appears as though Asia is recovering much faster than Europe. Why?

© DELFI (www.DELFI.lt) / Kiril Čachovskij

WELCOME & OPENING SESSION

WELCOME
03.12.2020

Karl Nehammer

Austrian Federal Minister
of the Interior

© BKA / Andy Wenzel

I am very happy to be with you today and to welcome you to the second day of the International Digital Security Forum.

This conference highlights many important topics which are at the heart of our agenda to make Austria a safer place.

Digitalisation and globalisation are rapidly changing our world.

Crime is increasingly shifting from the physical to the virtual world.

COVID-19 has sparked an upward trend in cybercrime.

The Austrian Ministry of the Interior is committed to fostering a safe digital environment.

We will double the number of cyber cops within the next years.
To support all this work, we will further develop the legal basis for cyber security, including new rules for online crime.

Recent events have shown that the fight against terrorism is our top priority.

We plan to develop an office for online hate content, where everyone can report “cyber jihadism”, in order to effectively fight radicalisation on the internet.

At the European level, we are working at the same time on the necessary tools to better fight terrorist and extremist content online.

Together we are strong, and we will make the digital world an enjoyable and safe place.

Today we shape the future of tomorrow. A tomorrow in which cybercrime will be in decline and online disinformation a thing of the past.

Our efforts today are vital if we are to ensure a prosperous, safe and democratic digital future.

I am pleased that international discussion is taking place in Austria, and wish you a successful conference.

Thank you!

Keynote

Arne Schönbohm

President of the Federal Office for Information Security (BSI), Germany

© BSI

Dear Minister of the Interior, dear colleagues and friends, it is a great pleasure to talk to you today. First of all, I would like to thank the organisers, the Austrian Institute of Technology and the Austrian Economic Chamber, and their partners, for the invitation and for making this event possible. Honestly, I would love to talk to you face-to-face today, but this year has shown us that the global community is able to continue its work and exchanges in new formats to protect our health and safety in such trying times as a global pandemic, which is really challenging.
As President of the German Federal Office for Information Security, it was beyond question to follow your invitation and contribute to the International Digital Security Forum Vienna.

The motto that our Austrian friends have chosen for this conference is “Security in times of pandemics and major global events”. I applaud you for choosing this title. I am very pleased that this conference will provide the opportunity to hear different views on pressing issues such as the challenges and abuse of virtual currencies and explainable AI, among others.

We need to discuss these matters together in a strategic way, because only together can we push for needed developments for the recognition of cyber security as a global goal.

The cyber security field has already gone through many changes in the past years. In Europe, the level of cooperation and coordination has grown enormously. Allow me to give you some examples from our European experience.

European examples

Let me start with the milestone NIS Directive, its current review and the Cybersecurity Act.

The first European cyber legislation came into force in 2016, with the NIS Directive. This was an important step for enhanced European cyber security of critical infrastructures. It also gave life to new forums for regular exchanges, as well as for exchanges regarding cross-border incidents.

Our overall experience with the implementation of the NIS Directive has been positive. An important success factor was undoubtedly the flexibility for Member States.

And I think Member States play a very important role here. Because even if we strive towards the same goal, the way to get there might have to be different depending on the situation you find yourself in. This flexibility is something we would like to preserve, while at the same time we also see elements that could be improved, that we should improve. I do not want to go into too much detail. The work to be done is extensive and will take longer than our Presidency of the Council of the European Union. So, it will be particularly interesting to see which ideas the European Commission will present at the end of this year.

For another important European milestone, let me jump back to 2019, when the Cybersecurity Act entered into force. The regulation is twofold: it serves as permanent mandate for our esteemed partner, the European Union Agency for Cybersecurity, ENISA, and laid the basis for cyber security certification on a European level. In my opinion, certification is a topic that offers many strategic possibilities for cyber security. It not only gives the possibility to discuss security standards for products, processes or services, but it also allows us to make a joint commitment on cyber security for consumers. Therefore, it was positive to see how this regulation, its new groups and processes came to life over the course of the past year and will continue to do so in the future.
From my experience, I can tell you that, within the EU Member States, we undoubtedly have extensive technical expertise and experience in various fields as well as a spirit of striving for innovation. From my point of view, it is of utmost importance that we leverage these resources to support each other, learn from one another and share best practices. We, as the BSI, the German national Cyber Security Authority, are ready to do so. We have more than 1,000 employees and we are able to support you, because together we are much stronger.

Report on the state of IT security in Germany 2020

Today’s cyber security threats are high. On 20 October this year, together with the Minister of the Interior, Horst Seehofer, I presented the “Report on the State of IT Security in Germany”. There, we made a few statements:

We are not yet living in a digitalised world. We are videoconferencing, we are holding different kinds of conferences and meetings in a digital format. But, if you are travelling by car, you still drive on your own. You are not taking an autonomously driven car.

Even if we are not yet living in a fully digitalised world, we see more than 1 billion malware programmes. We saw last year 117 million additional variants of malware. That is the current status. We know that since 2009, organised crime is earning more money with cybercrime than with drugs. Therefore, we think that we have a very tense level of information security.

We are successful in some areas. For example, we block 35,000 emails containing malware per month. We have prevented the German government from being severely attacked so far, but we have to do much more.
The case of a smart watch noted in our last report is a good example of our typical work. Researchers published a vulnerability concerning, among others, missing encryption between the corresponding app and the server of the manufacturer. BSI checked this, confirmed the vulnerability and contacted the manufacturer who solved this problem. BSI again checked the updated version. By doing so, we improved the security of the smart watch producer. We enhanced the security of the overall ecosystem in a digitalised way. And this is very important. This is something we should do in facing these challenges.

Cyber Security Conference on 9 November and security of IoT as focus of the German Presidency

Here, I can mention the “evergreen” finding that cyber threats do not stop at national borders. Cyber security is a collective effort – not just of a single nation – with the strengths of the nations and the national capabilities.

Therefore, I remember very well our conference that took place on 9 November in Berlin, and in a digital format, as part of the German Presidency of the Council of the European Union. We invited more than 400 guests, who participated virtually.

There, we had one pillar. This was the initiative on the cyber security of connected devices. Everybody in the industry is speaking about industry 4.0 and the Internet of Things. We have to make sure that this does not become an Internet of insecure Things. Today, a large number of devices do not even meet baselines of information security, but we are still willing to connect them.
This will generate a new threat level. Here, we have to counteract.

Let me give you
two examples of such vulnerabilities:

1) A classic example is attacks on insecure IP cameras. These often use standard passwords or allow weak passwords. Users and their families might be watched, which is a deep intrusion into privacy.

2) A while ago, in cooperation with internet providers, we at BSI contacted users who used their smart home base station completely unprotected in the internet. The affected devices had no access protection by default. This cannot be allowed to continue.

Engagement of BSI towards more cyber-secure products

In an ever more connected world, cyber security must be the basis for digitalisation, and not just a basis, but a precondition for a successful digitalisation. I cannot stress this enough, because this is of the utmost importance for us at BSI.

We identified a few problems. One problem is the so-called “time to market”.
With a short “time to market” - everybody tries to be as quick as possible – you probably do not meet minimum requirements for information security. This cannot be.

Therefore, it is very important that we are using security standards we already have for security by design, for example, ETSI IoT standard EN 303 645. At BSI, the work for international standardisation activities is a cornerstone, a pillar. I believe that the different Member States within the European Union should play a stronger role together with the European industry.

There are of course different national ideas addressing a so-called “IT security label”. We feel, for example, that an IT user should be able to identify how secure products are. This is important to us.

Closing remarks

Why am I telling you this? From my national experience, this is one take-away I would like to emphasise today: It is necessary to reach out to international partners and to foster exchange with all relevant stakeholders, but when exchanging, it is important to make pragmatic proposals that can bring you to the next step of integrated cyber security – whatever the technical field you are working in. Information security is a precondition for successful digitalisation.

A second take-away for a global outlook on cyber security is that the COVID-19 pandemic has produced challenges but also opportunities. We are still able to work and stay in contact with our loved ones, who might be living on the other side of the planet, because of digital solutions and innovations from the past decades. The increased demand for digital solutions must now be used to shift the paradigm of cyber security from a costly hurdle to a distinct economic advantage. It is our responsibility to make pragmatic and technically feasible cyber-secure solutions possible. BSI published different kinds of reports on securing your home office, on what should be the minimum standards regarding health products. These should be implemented right from the beginning.

With this in mind, I hope that we will continue our fruitful discussions today and thank you very much for being here. I wish us all a great conference and I am looking forward to seeing you next time, again in Vienna. Thank you very much.

CHALLENGES AND ABUSE OF VIRTUAL CURRENCIES

Speakers

Rainer Böhme
Professor for Security and Privacy at the University of Innsbruck

Haaroon Yousaf
Doctoral Researcher at the Initiative for Cryptocurrencies and Contracts (IC3), University College London (UCL)

Georgios Kappos
Doctoral Researcher at the Information Security Group, Department of Computer Science, University College London

Eljo Haspels
CEO at Cointel B.V.

Kamal Anwar
Associate Counter-Terrorism Officer, Countering the Financing of Terrorism (CFT) Programme, at the UN Office of Counter-Terrorism, New York

Host

Bernhard Haslhofer
Thematic Coordinator at the AIT Austrian Institute of Technology

Virtual assets such as Bitcoin can certainly be regarded as a disruptive innovation with the potential to transform the financial sector. However, we can also observe the flip side of this innovation, and see thatwith virtual currencies are also abused for criminal activities such as ransomware, ponzi schemes, money laundering, and terrorist financing. The goal of this session was to talk about possible measures that can help us to reduce the abuse of virtual assets and keep end users safe. For that we invited a panel of internationally renowned experts in this field and asked them for brief input statements. These were then followed by a panel discussion, which also involved questions from the audience.

Eljo Haspels, CEO at Cointel B.V., a virtual currency intelligence company located in the Netherlands, was the first speaker on this panel. He talked about strategies for enabling effective virtual currency intelligence and pointed out that, according to his experience, knowledge gaps at on the operational level, rapid technology development, as well as data availability and reliability are the main challenges customers are currently facing. The challenge for companies like Cointel lies in finding and connecting relevant data sources and in keeping up with technical developments. Therefore, he considers partnerships as being important to make sure that the world becomes a little bit safer.

Next, Haaroon Yousaf and George Kappos, researchers in the field of cryptoasset analytics at University College London, contributed a statement on the privacy of off-chain transactions in the Lightning Network, and presented three novel attacks that can exploit publicly available information about the network topology and its active nodes and channels in order to learn information that is designed to be kept secret. This shows that payment channels are not as private as generally assumed, but the traceability of transactions, as it is currently possible in public blockchains, will certainly remain a difficult challenge.

Rainer Böhme, professor of computer science at the University of Innsbruck and pioneers of cryptocurrency research, talked about possible designs of for Central Bank Digital Currencies (CDBCs). He presented the CDBC pyramid as a conceptual framework for aligning consumer needs with CDBC design choices. He concludes that the challenge of retail CDBC, if a central bank rolls it out, lies in getting it right from day one, and most technology is not ready before version 2.0.

Finally, Kamal Anwar, an Associate in the UN Office of Counter-Terrorism in New York, talked about countering terrorist financing through cryptocurrencies. He presented case studies of terrorist attacks involving cryptocurrencies, including the the Easter bombing in Sri Lanka, organisations like ISIS, Hezbollah, al-Quaeida, or the military wing of Hamas. He also pointed out that American neo-Nazi groups are early adopters of cryptocurrencies, and have raised approximately US$1.8 million so far. Their desire is to stay outside government controlled systems, which is often motivated by conspiracy theories.

The panel discussion was mostly centred around the evolution and novel forms of abuses, as well as general developments in the cryptoasset space, such as CDBCs, corporate currencies, stable coins, and emerging financial paradigms as we see appearing in the field of Decentralised Finance (DeFi).

TRUST IN COMPLEX CYBER-PHYSICAL ENVIRONMENTS, ORGANISED BY SBA RESEARCH
WEBINAR

After three years of research, the Austrian Flagship Project IoT4CPS used IDSF 2020 to present its research findings on establishing trust in complex cyber physical environments such as autonomous vehicles and connected factories. The webinar included Stefan Mangard's presentation titled, "Do you really think security is necessary?", followed by an overview of the project outcomes – "How to secure your autonomous vehicle and how to protect your supply chain" – given by IoT4CPS project leader Mario Drobics.

Do you really think security is necessary?

The megatrends of the last decades have fundamentally reshaped our IT landscape, and this transformation is far from complete. Our networks keep getting faster, while our hardware is continually becoming smaller, cheaper, and more powerful. In addition, software accounts for an increasingly large part of a product's value. While it was mechanical engineers who built cars in the past, in the future autonomous driving will put computer scientists in the driving seat of the automobile industry. This trend is mirrored elsewhere, whether for toys, manufacturing sites, or a vast range of products and industries we are familiar with today.

Current developments are leading to a change in business models, transitioning from selling products to selling services in the cloud. An app provider uses the hardware belonging to a cloud provider to manage data belonging to private individuals. In turn, a cloud provider's measurement data is collected on a customer's device and processed on the hardware belonging to a cloud provider. There are multiple parties with different interests and assets involved, not just in the cloud, but also on IoT devices.

A number of security challenges demand that we switch towards a data-centric view, as well as rethinking the way we build systems. Above all, security must be integrated into every product right from the design phase: as every product is becoming an IT product, specific and usable tools for their construction need to be established.

Insights into the challenges addressed in IoT4CPS:

- Security Design and Methods
  Interfaces between technological layers and modules are a central source of security vulnerabilities.

- Security Verification and Analysis
  As anybody can make security claims, proofing and providing a solid security argumentation for a system presents a major challenge.

- Security in the Product Lifecycle
  IT products are not built and then ignored, but require ongoing monitoring and updates.

How to secure your autonomous vehicle and how to protect your supply chain

Over the past three years, the IoT4CPS project has been working on the challenges arising from the use of information and communication technologies (ICT) in real industrial environments. In addition to cyber security issues, this also includes aspects of availability and (physical) security, from the design to the operation of the plant. Consequently, the project consortium developed methods for the joint consideration of safety and security over the entire life cycle. The topic of security was considered at all levels, from the sensor through the communication interfaces to the networked systems. The suitability of the innovative project results for use in networked industrial production facilities and in the field of networked vehicles was evaluated using various industrial demonstrators.

Technical aspects of safe IoT

A high degree of trust between the system components involved must be ensured if the potential of applications for automated driving with connected vehicles, and of trustworthy, robust and cost-efficient Industry 4.0 concepts, are to be fully exploited. This includes the integrity, authenticity and confidentiality of information, as well as the adequate protection of production data and intellectual property. In the past, industrial plants were rarely ever adapted after commissioning. Today's networked digital plants require a much more extensive security management.

The end-to-end security of IoT in cyber physical constellations (interactions between digital devices and their physical environment) demands the use of combined safety & security approaches, starting in the design and development phase and across all levels of the system architecture, from the physical, network and platform levels to the applications. In addition, comprehensive verification and security analysis during operation, as well as IoT lifecycle management, are necessary to ensure security over the long operating life of industrial plants.

Industry 4.0 demonstrators

In order to demonstrate the technical achievements of the project and the advantages of the IoT4CPS developments in design and reference architecture in a showcase, the consortium developed two Industry 4.0 demonstrators that integrated various technical components resulting from the research work. These prototypes illustrate how IoT4CPS solution approaches can be applied in a wide variety of smart industrial environments, and clearly demonstrate how industrial process efficiency can be increased by means of trustworthy connectivity and, more generally, how the time to market along the entire product life cycle can be accelerated through digitalisation. The first demonstrator facilitates bidirectional connectivity for the industrial testing of components in vehicle manufacturing, facilitating process automation, optimising productivity, and supporting predictive maintenance. The second demonstrator uses virtualisation technologies to securely integrate existing equipment into a networked production environment. In addition to innovative concepts, special devices developed in the project were used, enabling a secure connection of industrial equipment (machines, robots, production lines). This results in the creation of a virtual factory, featuring 'security by isolation'.

Speakers

Mario Drobics
Head of Competence Unit Cooperative Digital Technologies, Center for Digital Safety & Security, AIT Austrian Institute of Technology

Stefan Mangard
Professor and Head of the Institute of Applied Information Processing and Communications at Graz University of Technology

Philipe Reinisch
Project Manager IoT4CPS, AIT Austrian Institute of Technology, Founder of SILKROAD 4.0

Julia Pammer
Project Manager at SBA Research

EXPLAINABLE AI

Speakers

Sepp Hochreiter
Head of Institute for Machine Learning at the Johannes Kepler Universität Linz

Allan Hanbury
Professor for Data Intelligence at the Technical University of Vienna – Institute for Information Systems Engineering

Jochen Borenich
COO at Kapsch BusinessCom

Mariarosaria Taddeo
Deputy Director of the Digital Ethics Lab at the Oxford Internet Institute, University of Oxford

Host

Willibald Krenn
Thematic Coordinator at the AIT Austrian Institute of Technology

Many AI-based systems are built as 'black-box' systems without anyone understanding how exactly they derive decisions or providing an explanation of how a certain outcome was reached. The IDSF session on Explainable AI (X-AI) looked at the business, research, and philosophical importance of explainability in the context of AI, with Mariarosaria Taddeo, Sepp Hochreiter, Allan Hanbury, and Jochen Borenich sharing their insights and participating in a panel discussion.

Mr Jochen Borenich, Board Member of Kapsch BusinessCom AG, started the session by pointing out that, due to digitalisation, more and more data is available and the speed at which decisions must be taken increases. So, the question becomes, who is taking these decisions? Is it a human, a human with support of machines, or machines alone? He emphasised that – regardless of who takes a decision – the need to understand why a certain decision has been taken remains, and that mankind will only be able to cope with the large amount of data with the help of AI. So, fostering trust in AI is an important business goal.

He identified three areas in which Kapsch is working on AI-based solutions today: manufacturing to increase operational efficiency and optimise energy consumption, the medical domain where Kapsch is active in developing AI-based technology for assisting humans in image analysis in digital pathology, and cyber security. To corroborate the importance of AI in the cyber security domain, Mr Borenich shared the example of a Kapsch customer having several million events over the course of a couple of months that led to more than 200k alarms, of which 60k were critical, leading to 19 critical incidents. For the analysts in the cyber defence centre, AI technology is important in order to be able to concentrate on the 19 incidents, rather than having to go through 200k alarms manually.

Mr Borenich closed by saying that customers of products that are targeted at humans are especially sensitive to explainability, while customers of products that are not directly targeted towards humans (e.g., security, manufacturing) currently care more about the performance and the reliability of AI solutions and to a lesser extent about explainability. Even so, these customers will not accept black 'AI boxes', so that open tools, open source, transparent training data, and high statistical quality are all important. In summarising, Mr Borenich said that "AI is the steam engine of the 21st century" and that we should use it to increase productivity in an explainable way.

Prof. Sepp Hochreiter, Head of the Institute for Machine Learning at the Johannes Kepler University of Linz, shared recent scientific developments, also referring to the book "Explainable AI: Interpreting, Explaining and Visualizing Deep Learning" as a source of further information. He identified three important topics with respect to X-AI: (1) building up trust, (2) verification and certification, and (3) avoiding bias.

Regarding trust in AI systems, Prof. Hochreiter pointed out the 'Clever Hans' fallacy that can also befall AI systems. 'Clever Hans' predicts correctly, but for the 'wrong' reason. A popular example is an AI classifier that learns to classify pictures of horses, but actually learns that all the training images with horses it has been given have a copyright watermark. Consequently, it actually learns to recognise the watermark, rather than the horses. Contribution analysis, in which parts of the inputs to the AI system (e.g., pixels in an image) are examined with respect to their influence on the outcome/decision, is a useful tool for countering this phenomenon.

For systems that receive rewards for achieving certain goals, contribution analysis can be seen as a credit assignment problem: upon receiving some reward, previously performed actions are assigned credit. The challenge here lies in the fact that strategic decisions lead to delayed reward, which makes it hard to assign credit to actions responsible for achieving the reward. Prof. Hochreiter's team works on reward redistribution algorithms that give reward when the expected return changes, aiming at the goal of all future expected reward being zero. Given such a reward redistribution, it will – among others – explain the prediction (which inputs contributed), explain the consequences of actions (what happens in future), explain the strategy or policy, and explain the performance of an agent (why did it achieve a goal).

Prof. Allan Hanbury, Professor for Data Intelligence at the Institute for Information Systems Engineering at TU Wien and Co-Founder of Contextflow, asked "Who is the explanation for?", because different audiences will require different explanations. To illustrate his point, he took explanations from Amazon's shopping recommendations and Google Ads and compared them with examples taken from medical and legal domains, in which decisions have ramifications for people.

In his first example, Prof. Hanbury showed a system offered by Contextflow to support radiologists in their work. The system is a deep learning-based tool that, when presented with pictures, e.g., from computer tomography, will look for unusual patterns and find similar images in a curated and labelled dataset. It will then present the found patterns, their location and distribution next to the set of similar images from the labelled dataset to explain why the radiologist should examine them further. The system will also look for diagnosis guidelines, e.g., on how to do a differential diagnosis, and present this information to the radiologist as well. "At the end the radiologist makes the decision and writes a report," Prof. Hanbury commented, also saying that the system is in active use and radiologists like it as the system comes up with relevant information and presents it in a way it is easy for them to work with, allowing them to dig deeper, if necessary.

The second example was based around the needs of building inspectors. Before a new building in Vienna is issued with permission for construction, the plans are checked against the building code of Vienna to see if all legal requirements are fulfilled. In a recent research project, Prof. Hanbury's team is trying to automate this task. To do so, Vienna's building code is converted into a form that allows automated reasoning (deontic logic) with the help of natural language processing. In a next step, the plans are analysed, and identified elements in the plan are checked against the digitised building code. For any element in the plan, the system can give an explanation (reasoning) why it is (not) in accordance with the building code. However, different representations are necessary depending on who the explanation is intended for, e.g., NLP experts, logic experts, building inspectors.

Summing up, Prof. Hanbury stated that explanations are generally possible but not always useful and that solid explanations are needed in domains such as medicine and legal. Finally, system developers need to think carefully about who the explanations are for.

Prof. Mariarosaria Taddeo, Deputy Director of the Digital Ethics Lab at the Oxford Internet Institute, University of Oxford, highlighted the potential AI offers for supporting human experts, e.g., in mitigating cyber attacks. She also pointed to numerous initiatives (US executive order on AI, EU Commission Cyber Security Act and Guidelines for AI, the IEEE 2017 report on standards for AI in cyber security) aiming to foster trust in AI. However, she warned that this would mean trusting a technology we have little control over, in so far as, given the input and architecture, we cannot predict the outcome, nor can we explain how this output has been delivered, whether it has been produced in the right way. So, trust in AI is problematic.

Trust, from a conceptual point of view, is a form of delegation with no control and is often based on the assessment of the trustworthiness of the trustee. Trustworthiness itself is a measure of (a) predictability of behaviour of the trustee and (b) the risk for the trustor if the trustee behaves differently. Hence, the trustworthiness of AI can only be seen in context: humans will have a much harder time trusting an AI system making decisions that lives depend upon, than a system presenting shopping recommendations.

Looking at the first factor, predictability, AI-based systems are challenged by attacks such as data poisoning, tempering of categorisation models, backdoors, and others aiming to gain control over the AI system. The current countermeasure is to build robust AI systems. However, Ms Taddeo warned that this is an intractable problem as the source of perturbations is astronomically large and guaranteeing robustness against all these simply is infeasible. Hence, she concluded that "trusting AI in cyber security is conceptually misleading and operationally dangerous".

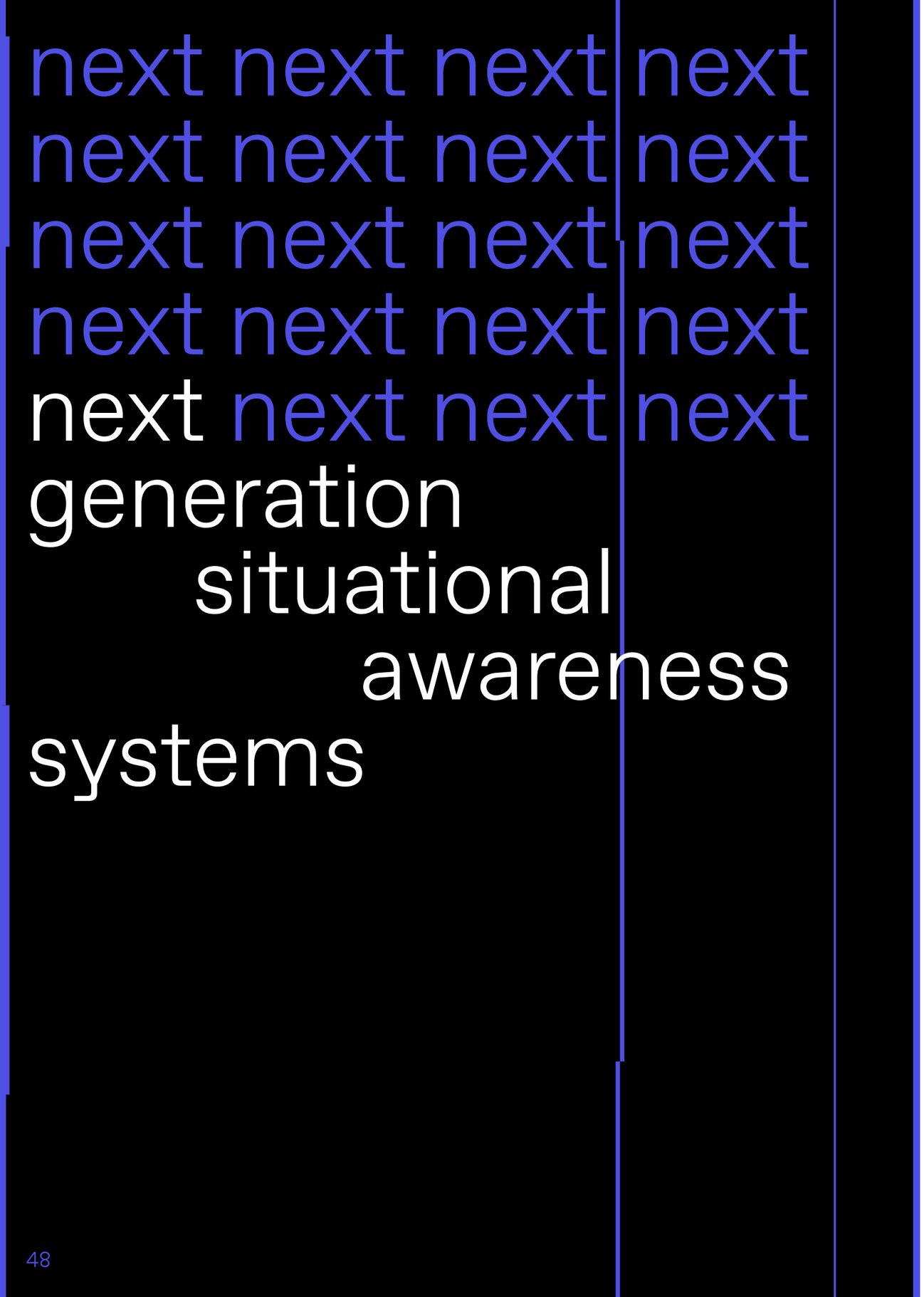
Her proposed solution is to move from a trust-based approach to a reliability-based one that fosters mandatory in-house development, adversarial training standards, and parallel and dynamic monitoring, with the help of digital twins, for example.

Some of the panel's conclusions:

Standards will be important for the development of AI-based systems, not only as they allow certified AI systems but also because society will decide on the values embedded in the standards. Explainability may not be the only way of increasing trust in AI systems, which might come with dangers such as trusting blindly or too much: mitigation of risks due to a lack of explainability can probably also be overcome through auditing, co-creation, and processes that ensure systems are improved over time, preventing the repetition of past mistakes. While requiring explainability may be technically possible, it may come at the cost of the overall system being less performant than without explainability. From a business perspective, a system that explains itself might give away business secrets which could be detrimental in certain business cases. In any case, it is important to bear in mind who the explanation is intended for, and to what extent it is necessary. The panel expects consumers to drive the trend towards X-AI, similarly to the GDPR.

Regarding classic versus deep learning-based approaches and explainability, it was agreed that both presented challenges: a long list of logic formulae is as challenging to understandability as complex neural networks. Complex systems should therefore have some hooks for experts, allowing them to check that no bias has crept in. The performance of AI methods also needs to be improved: while they work well at a sensory level (e.g., image/speech recognition), improved methods are needed for higher-level reasoning (cf. system 2 deep learning) or learning from sparse data.

There are many areas in which AI systems will hopefully improve productivity, such as relieving medical staff from repetitive, machine-like tasks, supporting building inspectors, increasing the competitiveness of manufacturing, or even helping society tackling big challenges such as climate change. At the time of writing it is unclear whether AI can fulfil these expectations. What we do know, however, is that people will just ignore AI systems if they consistently produce incorrect results. Let's hope future systems can be trusted.



Speakers

Georg Aumayr
Head of Research and Innovation
at Johanniter-Unfall-Hilfe in Österreich

Harald Felgenhauer
Director of the Systemic Foresight Institute, Austrian Federal Ministry of the Interior

Christian Resch
Managing Director of the Disaster Competence Network Austria

Niek Mestrum
Business Development Manager Security and Defence at SAS Institute GmbH

Marcel Van Berlo
Programme Coordinator at the TNO

Karin Rainer
Project Portfolio Manager at the AGES Austrian Agency for Health and Food Safety

Host

Georg Neubauer
Thematic Coordinator at the
AIT Austrian Institute of Technology

Major events, including natural disasters such as flooding and wildfires or pandemics such as COVID-19, require perception and understanding of the environment and origins of the specific event. Building, maintaining and sharing situational awareness is fundamental to ensuring interaction and coordination of the various stakeholders, such as public authorities, crisis managers and first responders.
In this light, the Next Generation Situational Awareness Systems session was a journey through the experiences of multiple stakeholders in the crisis and disaster management community, encompassing crisis managers, first responders, researchers and key players from industry, to highlight multiple facets of situational awareness.

From the perspective of AGES, it is essential to have a timely, reliable and easily accessible situational awareness system in order to act as a central communication hub between national service providers and the public. Karin Rainer from AGES reported that, by the end of February 2020, the first COVID-19 cases had been confirmed in Austria. At this stage, the Corona hotline was installed and heavily used. The unclear development and the dynamically changing situation required low threshold, reliable information to be made available to the population. A call centre was quickly set up, but the logistics of dataflow were problematic, and the quantity and requirements of information seekers were very demanding. Harald Felgenhauer from the Austrian Ministry of the Interior reflected on the management of the COVID-19 crisis. The majority of stakeholders and experts did not expect such an evolution of the crisis, and the question arises of what lessons can be learned from this pandemic. Mechanistic models and linear thinking are not suitable for managing such complex, interconnected risks. New risk management methodologies are needed, and can be achieved by answering central questions such as the real status of current knowledge or the relevance of past experiences to the situation at hand, in order to obtain reliable situational awareness for decision support.

Marcel van Berlo from TNO, the technical coordinator of the European flagship project DRIVER+, showed two beneficial project outcomes for improved situational awareness, namely the Portfolio of Solutions and the Crisis Management Innovation Network Europe. Both solutions continue to be operated beyond the lifetime of the project. They ensure availability of emerging solutions related to situational awareness, help to close existing crisis and disaster management gaps by identifying adequate solutions, and allow networking and sharing of experiences. The expectation of a first responder on the outcomes of research projects was presented by Georg Aumayr from the Johanniter Austria accident assistance organisation. He stressed that research needs to follow a user-centred approach. Solutions providing situational awareness should ensure an optimised, simple view of the status of an event, information about the availability of resources, and finally provide decision options. Key targets are always increased awareness, support of operations and finally reduction of risks and threats for rescue units and victims. The road from awareness to competence building was presented by Christian Resch from the Disaster Competence Network Austria. He stressed the importance of ensuring adequate situational awareness within the population. To enhance resilience, service providers need to follow human-centred approaches, to develop solutions that are tailored to users' needs. The human factor makes it imperative to take risk perception of the population into account and to design adequate risk communication strategies.

Application of advanced analytics is a central element in achieving situational awareness from the solution provider perspective. Niek Mestrum from SAS sketched the path from data to intelligence by the application of analytics. A requirement is to understand the environment, the situation and the ability to make projections of a future status, as well as needs. Understanding a situation implies different types of intelligence methods, of variable degrees of complexity, such as anomaly detection, predictive modelling, network analysis and text mining. Advanced analytics can be applied in different contextual frames, such as applications for police, military or humanitarian perspectives.

“FROM AUTOMATED DATA ANALYSIS TO MOBILE FINGERPRINTING – MAKING AI WORK FOR YOU”, ORGANISED BY T3K

Webinar

Speakers

Joachim Müller
Sales Director Europe at T3K

Gareth Balance
Product Manager LEAP

Jürgen Mathwich
COO T3K

T3K’s focus is the practical use of advanced AI systems, especially image and video analytics, and using camera images for biometric data acquisition. Therefore, we are highlighting two of our products: LEAP (Law Enforcement Analysis Platform) and Biocapture.

LEAP is a quick, automated tool that aggregates and reports data from mobile device extractions that can point to an individual’s identity and activity, such as their communication, location and browsing patterns, account data and phone use. More importantly, an AI-embedded analysis of images and videos from the device automatically detects content such as ID cards, licence plates, weapons and military equipment, terrorist or extremist symbolism, and more.

Using a combination of watchlists, multilingual OCR, face recognition, multilingual audio keyword spotting and automatic detection of extreme content in images, videos and documents quickly provides actionable intel and case prioritisation. This initial AI-enhanced first-look into a vast amount of digital content saves time and provides focus much more efficiently than relying on traditional manual analysis and review tools.

Biocapture also uses AI technology, in this case making available fingerprints captured with a standard smartphone camera ready for matching against existing biometric fingerprint databases. Biocapture allows identity checks on the go, in the field, and does not rely on auxiliary devices, thus eradicating challenges seen with other technologies such as surface debris and hygienic issues, which only increase during the current SARS-CoV-2 pandemic, as well as expensive hardware and logistics.

The flexible integration of an available software development kit (SDK) into existing apps or other upstanding systems is enabled, allowing installation on COTS devices, such as smartphones or tablets.

The location of fingers is detected and visualised using augmented reality. A built-in visual quality assessment feature shows a live preview of the fingerprint quality, based on NIST NFIQ 2. The capturing process will stop automatically as soon a certain quality threshold has been reached.

AI and smart technology are commonly used buzzwords, but making use of them to really work for the users and make their day-to-day business easier is our goal and objective.

CYBER SECURITY – Capability Building in Times of Covid

Speakers

Bernd Pichlmayer
Policy Adviser at the Austrian Federal Chancellery

Trent Nelson
Senior Information and Computer Security Officer at the Division of Nuclear Security, Department of Nuclear Safety and Security, International Atomic Energy Agency (IAEA)

Álvaro de Lossada Torres-Quevedo
Head of Section on Logical Security, Center for Cybercriminality at the Spanish National Police

Alexander Janda
General Secretary at KSÖ Kuratorium Sicheres Österreich

Thomas Braun
Head of the Cyber Security Section at the Office of Information and Communications Technology, United Nations, New York, USA

Host

Donald Dudenhoeffer
Cyber Security Research Engineer at the AIT Austrian Institute of Technology

Building cyber security capability and maintaining operational readiness has been challenged by COVID-19. With so many workforce activities going virtual, including training and exercises, there are legitimate questions about how to effectively operate and maintain a sufficient level of security in the current chaos. This session discussed current operational challenges as well as recommendations for moving forward. The discussion focused on both national perspectives from Austria and Spain, as well as international perspectives from the United Nations and the International Atomic Energy Agency.

National perspective

Mr Bernd Pichlmayer opened the session by describing his observations while working as an adviser to the the Federal Chancellor of Austria on cyber security. While the COVID crisis has been a significant challenge for the Chancellery, as it has been for all states, in terms of the impact on cyber security, it is only one of many ongoing risks presented by digitalisation. The more society is digitised, the more dependent we become on digital technologies, further increasing the importance of cyber security. Many of the challenges faced by the Austrian Chancellery are similar to those faced by other states and organisations. They include, firstly, the interdisciplinary nature of cyber security. Governments consist of multiple ministries, each with its own functions and responsibilities. Cyber security essentially overlaps all competencies within a government. Furthermore, multiple ministries may have cyber security responsibilities, such as the Ministry of the Interior and the Ministry of Defence. This can lead to parallel structures and competing resources, resulting in less than efficient overall efforts. With regards to resources, especially experts in cyber security, further challenges exist in that they are a rare commodity and expensive. Both are impediments for their inclusion in public service.

A hard reality of governmental and organisational transformation is that it often actually only happens after a precipitous event: in the case of cyber security, after a consequential cyber attack. Such events raise awareness of the potential impact of a cyber event, as well as the need to strengthen protection and resilience to such attacks. The complexity of societal digitalisation requires building awareness and knowledge, but also the ability to make the complexity of cyber space understandable for government entities, businesses, and the broader society,

i.e. translating the digital world to the real world. The digital community, including cyber security, must become better at communicating to the larger stakeholder community in an operationally relevant language.

From a government perspective, what are some key elements moving forward? Cyber security affects everyone, and so everyone must develop some level of awareness, supported by central rules and guidelines. There continues to be a growing need for organisations to share information regarding cyber attacks and cyber compromise. In the EU, this has been facilitated by the GDPR requirement for organisations to report when personal data is stolen. The GDPR made reporting an obligation, where in the past organisations may have been reluctant to do so. Ongoing initiatives are needed to raise awareness of cyber risks. Humans are still the biggest contributors/causes of cyber compromise. Changing at-risk cyber behaviours remains a challenge. Finally, it should be noted that cyber security is a process: it is a journey that requires persistence and adaptability.

International efforts and challenges

Mr Thomas P. Braun next shared the perspective of the United Nations and some of the challenges and adaptions they have seen to maintain effective and secure operations in a virtual workspace. The UN has offices and a presence around the world, with a global workforce of over 50,000 people. It is a multilateral intergovernmental institution whose main constituents are Member States, i.e. governments. The primary interface mechanism between the UN and states are delegates, and interactions with the ministries themselves through conferences of the main bodies and working groups. Almost overnight, the UN has had to shift to a virtual framework to continue its operations. Two observations from this transformation are, firstly, that this crisis has highlighted the reliance of organisations and society on ICT, and the need for well-designed and implemented ICT solutions that provide tailored and secure functionality. This can be seen when conducting UN intergovernmental meetings that require simultaneous interpretation in a secure and highly confidential environment. Previous video conference solutions existed prior to COVID-19, but did not fit the scaling and security requirements. This past year, however, has seen many improvements as lessons have been learned. In these environments access control and identity management are essential security elements. An ongoing challenge is often user acceptance of important security concepts. This results from both a lack of awareness of the given technology and its potentially complicated implementation. Users often chose the simple, known, but less secure solution.

Another security challenge is that, in the shift to 'working from home', many have been forced to use personal devices to conduct official business. In this case, personal devices often do not have the rigorous security controls offered in an office environment. Security monitoring has also been challenged in that, instead of providing monitoring and analysis of network traffic residing on internal systems, it is a matter of trying to monitor thousands of remote endpoints. The UN has developed ad hoc measures to enhance security in this situation, but this came at the price of additional resources, including the need for additional technical capabilities for system administration and support to a now almost totally virtual workforce. Technologies for secure remote interactions exist, but unfortunately such solutions are not universally implemented and may suffer from scaling issues. The security model of working within a protected corporate network must be replaced with a defensive strategy and model that supports a virtual and distributed workforce.

The International Atomic Energy Agency (IAEA) is another multilateral intergovernmental institution providing support to constituent Member States. Mr Trent Nelson provided an overview of the role of the IAEA's Division of Nuclear Security (NSNS) in their mission to support Member States in enhancing national programmes of nuclear security, including the development of cyber security programmes for nuclear and other radiological material infrastructure. NSNS also seeks to strengthen international cooperation in an effort to enhance nuclear security globally. Key components of implementing their mission include the conduct of conferences, technical meetings, and training courses. Information sharing and collaboration building is a cornerstone outcome of these activities. The COVID-19 situation has led to the postponement of 18 events and the requirement to develop and implement new approaches to meeting Member States' needs. This has included the development of the NucSec-Cyber Webinar Series. Lessons learned in conducting these virtual engagements include the need to enhance the experience of participants through the implementation of embedded surveys, scenario-based learning, group breakouts, and hands-on exercises that can be conducted virtually.

Technical and security challenges that have been encountered include limited remote access for all desired participants, limited endpoint security, increased file sharing and screen sharing, and increased reliance on third-party support and maintenance.

Cyber crime

The COVID-19 crisis has dramatically increased reliance on and use of ICT by the remote workforce. The new norm of working from home as well as the emotional tolls of COVID-19 have laid the ground for criminal activity which exploits both the new workplace environment and personal fears/anxieties. Mr Álvaro de Lossada Torres-Quevedo provided an overview of cybercrime and the current trends as seen by the Spanish National Police. Some of the activities directly related to COVID-19 include cyber attacks specifically targeting the healthcare industry, massive fraud campaigns related to COVID-19, and the identification of over 500,000 internet domains related to COVID-19 of which more than 50,000 were found to be malicious. It should be noted that the impact of many attacks occurring during this time may not become evident until a later date. The criminal actors, after compromising the network, could remain dormant until a future opportunity presents itself. Since the start of the COVID-19 crisis, Spain has seen a rise in ransomware attacks. Diligence is needed more than ever to protect corporate ICT infrastructure as the office network is now connected to thousands of remote endpoints.

Going forward, key elements needed to combat these trends in cyber crime include highly technical training for law enforcement and cyber security stakeholders to counter growing cyber crime capabilities, adaptive measures and tools to continually adjust to the changing threat, enhanced cooperation among both national and international law enforcement stakeholders, and private-public partnerships.

Collaboration

As the previous discussion points have illustrated, the COVID-19 crisis has had a significant impact on the workplace and societal norms, including a growing reliance on distributed ICT infrastructure. Mr Alexander Janda pointed out, however, that while COVID-19 has been a humanitarian and economic disaster, other areas of core infrastructure such as electrical power, water, and transportation have remained functional. The impact of COVID-19 on digital systems has been a secondary effect. Governments and organisations must also consider and prepare for cyber events that directly impact other infrastructures which place people, organisations, and even states at risk.

Cooperation and collaboration frameworks need to be established and exercised at all levels of preparation and incident response. Train and prepare: cyber security exercise and cyber event simulations are needed to train the relevant stakeholders and associated processes. Who are the stakeholders? Cooperation and collaboration involves multiple levels of stakeholders and brings forward the need for public-private partnerships and networks. Crisis management should be a framework capability that is exercised. The COVID-19 crisis saw the mobilisation of the research community on many fronts, and the rapid operationalisation and integration of cutting-edge technology to support crisis response. This same openness needs to be realised with digital technologies, with due consideration to security and personal rights.

Following Mr Janda, Mr Donald Dudenhoeffer noted that while technology-based, cyber security was very human-centric in its realisation. While discussion in the panel identified many of the technological challenges regarding implementation and security of the new 'virtual' norm, significant discussion also centred on the aspects of awareness, building secure workforce behaviours, training, collaboration and cooperation, all of which rely on human interaction. Likewise, cyber security involves partnership. Especially when engaging national and international stakeholders, one needs to develop trust, share information, and build unity of effort. Before COVID-19 and the reality of near total virtual engagements, these conversations often commenced with a cup of coffee or a beer. Those interactions are gone, at least for now, replaced by a video feed on the screen. In the present environment, we must strive to develop innovative ways to maintain engagement, enhance capacity and build community.

Conclusion

The growth of digitalisation in our society is set to continue. Crises like COVID-19 will continue to occur and change or mould the new 'normal', whatever that will be. Governments, organisations, and even societies must have the adaptability and technological tools to foster resilience. To build for the future, collaboration and cooperation is needed among an array of diverse stakeholders. Discussions for tomorrow's crises must happen today. We must learn from the experiences of COVID-19 and prepare for the next crisis, whatever form it takes. Crisis management and adaptability is a necessity. Research is a cornerstone, but we must have the ability to rapidly as well as responsibly operationalise research to meet urgent requirements. The future holds more digitalisation, more virtualisation, more remoteness. Challenges such as cloud structures, authentication, identity management, data protection, and data privacy will need to be addressed.

At the core of any future solutions and challenges is the human: the end user, the operator, the maintainer, the policy maker. Programmatic efforts are required to build awareness, sustain competencies, and translate the complexity of a digital world to operational elements.

Alexander Janda, Donald Dudenhoeffer

CYBER SECURITY – Technology and Security in the Age of Pandemic

Speakers

Friedrich Teichmann
Brigadier-General, Director of the Geospatial Institute, Austrian Armed Forces at the Ministry of Defence (BMLV), Austria

Fernando Puerto Mendoza
UNOCT, Office for Counter-Terrorism, Programme Management Officer, Cybersecurity and New Technologies Unit

Kai Rannenberg
Chair of Mobile Business & Multilateral Security at the Goethe University Frankfurt, Germany, Coordinator of the CyberSec4Europe Competence Network

Rafal Jaczynski
CSO at Huawei, CEE & Nordics at Huawei Technologies

Arne Schönbohm
President of the Federal Office for Information Security (BSI), Germany

Marie-Line Billaudaz
UNODC, Cybercrime Officer at UNODC Cyber Program at the United Nations Office on Drugs and Crime

Gert Seidl
Federal Ministry of the Interior (BMI), Cybercrime Competence Center at the Criminal Intelligence Service, Austria

Host

Helmut Leopold
IDSF Initiator, Head of Center for Digital Safety & Security at the AIT Austrian Institute of Technology

Technology and Security in the Age of Pandemic: international cooperation, cooperation between industries, CISERTs, incident and emergency response

The digitalisation of almost every area of our life has changed the rules of the economy and many mechanisms of our society at an impressive pace. This transformation has been enabled by modern information and communication technologies (ICT) in combination with the networking of nearly everyone around the globe. This transformation process is gaining further momentum through the networking of numerous physical objects, rapidly establishing the Internet of Things (IoT). These developments offer huge potential for creating new applications, businesses and value streams.

At the same time, the nature of threats to our digital systems has also radically changed and intensified. As more and more of our physical environment becomes digital and connected, our vulnerability grows, threatening not only IT systems, but also our physical infrastructures and personal privacy. Cyber crime, organised crime and cyber terrorism have gained new momentum for attacking the sovereignty of our systems and our lives.

The pandemic has changed cyber security threat scenarios

As a consequence of the Coronavirus in particular, work processes as well as private communications have increased our dependency on virtual technologies and the communications infrastructure. This shift has also brought the need for an evaluation of security requirements and for adaptive technology solutions that provide flexibility to organisations in these chaotic times.

The pandemic has also dramatically changed the threat environment. Pandemic-related cyberthreats are increasingly targeting new stakeholders, such as those in the medical domain. There has been an increase in phishing campaigns and malicious webpages and web domains, attacking the growing number of online users of communication and ecommerce services, as well as an increase in ransomware attacks, fraud attacks, and unauthorised remote access targeting businesses, critical infrastructure providers and even governmental stakeholders. In addition, an increase in propaganda, violent and extremist narratives and disinformation (i.e., fake news) related to COVID-19 is challenging individuals as well as our society as a whole. Finally, new technologies are further changing threat actor capabilities and thus also threat scenarios. Radical groups and terrorists are moving away from traditional social media platforms and turning instead to encrypted platforms, cloud storage services, and even gaming platforms.

The pandemic has highlighted the increased vulnerabilities of society to new and emerging forms of terrorism, such as misuse of digital technology, cyber attacks and bioterrorism. This was also noted by the UN Secretary-General, António Guterres, on 6 July 2020 [1] [2].

Vulnerability of our digital systems

It is also important to note that new challenges, not yet considered, are emerging.

We must gain a fundamentally new understanding of the implicit vulnerabilities of software, potential weaknesses in the usability of human-machine interfaces, and the limited awareness and skills of users of emerging technologies, in addition to operational vulnerabilities.

Furthermore, system dependencies and monopolies are jeopardising the correct functioning of our digital systems. This is exemplified by the vulnerabilities of our Global Navigation Satellite Systems (GNSS). Nearly all communication systems on our globe are dependent on the availability and accuracy of global satellite systems. In addition to interference due to solar activities, cyber attacks on GNSS infrastructures and spoofing attacks on end users are posing a growing threat to which we must pay much more attention in order to protect our systems [3].

The new threat landscape demands new answers

Research and implementation efforts must focus on building greater resilience into our systems considering this new threat landscape. A growing challenge and a crucially fundamental problem, however, is the increasing issue of scalability: for example, the reported number of online child sexual abuse images and videos has grown to upward of 20 million in Q4 of 2020, exemplifying the scalability problem [4]. Building countermeasures needs a holistic approach on a global scale; no country alone can be successful. An example of a successful cooperative initiative among law enforcement organisations and IT security companies is “No More Ransom” www.nomoreransom.org. This cooperation maintains a platform to increase the effectiveness of fighting ransomware cyber attacks. In addition to providing technical services to help victims, the platform also aims to educate users on how ransomware works and what countermeasures can be taken to effectively prevent such attacks [5].

The changing threat landscape requires a new perception of what constitutes critical infrastructures, of global responses through dedicated communications strategies, the need to strengthen the resilience of critical infrastructures, and additional international coordination and information sharing, such as the cooperation among CERTs and law enforcement online investigations. At the same time, however, it is essential to build countermeasures which respect universal human rights, giving particular emphasis to freedom of expression and the right to privacy.

New solutions for cyber security countermeasures, safety and security by design approaches, and privacy preserving system solutions are being investigated and developed by the global R&D community. However, enhanced partnership is needed. Such collaboration among cyber security stakeholders, e.g., the R&D community, industry and governmental stakeholders, is exemplified by the four European cyber security competence networks: CyberSec4Europe cybersec4europe.eu, CONCORDIA www.concordia-h2020.eu/, ECHO echonetwork.eu, and SPARTA www.sparta.eu [6]. More national, regional, and international efforts like these are essential.

We need greater cooperation between science, research, industry, NGOs and governmental stakeholders

Cyber security is intrinsically tied to a challenging environment: rapidly evolving technologies, newly emerging threats, constantly changing legal frameworks and national/international policies, and finally a global market facing transnational threats.

These challenges can overwhelm a single enterprise, and demand global cooperation among stakeholders including RTOs, universities, industry, infrastructure operators, and public authorities. Building a cyber-resilient society requires a holistic approach involving all stakeholders.
In conclusion, key actions moving forward include:

1. Raising awareness: expanding knowledge and understanding of the challenges and threats;
2. Developing scalable capabilities, competences, tools and processes by building partnerships; strengthening national, regional and international collaboration, including the sharing of information and good practices, both in the public and private domain;
3. Focusing on capacity building activities for critical system operators as well as governmental stakeholders through initiatives such as virtual training environments;
4. Supporting ongoing research to build capability to keep up with the evolving cyber threats, focusing on safety & security by design and implementing new encryption concepts for implementing privacy by design in our digital systems; and
5. Encouraging infrastructure operators to develop technology management capabilities, such as minimising the reliance on sole source technology providers in a global context by building multi-vendor architectures and structures for federated services.

References

[1] Fernando Puerto Mendoza, Adapting to the COVID-19 era: United Nations capacity-building work in the fields of counter-terrorism, cybersecurity and new technologies, presentation at the IDSF 2020, December 2–3, 2020.

[2] Mendoza & Nelson referring to https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[3] Friedrich Teichmann, SatNav and Secure Position-Navigation-Timing (PNT): The Basis for a Secure Digital Future, cybersecurity and new technologies, presentation at the IDSF 2020, December 2–3, 2020.

[4] Marie-Line Billaudaz, presentation at the IDSF 2020, December 2–3, 2020.

[5] Gert Seidl, presentation at the IDSF 2020, December 2–3, 2020.

[6] Kai Rannenberg, Cyber Security – Technology and Security in the Age of Pandemic, presentation at the IDSF 2020, December 2–3, 2020.


#IDSE

HOSTED AND ORGANISED BY

IN COOPERATION WITH

Federal Chancellery Republic of Austria

Federal Ministry Republic of Austria Europe, Integration and Foreign Affairs

Federal Ministry Republic of Austria Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry Republic of Austria Agriculture, Regions and Tourism

Federal Ministry Republic of Austria Defence

Federal Ministry Republic of Austria Interior

SUPPORTED BY

Federal Chancellery Republic of Austria

Cyber Sicherheit Plattform

Federal Ministry Republic of Austria Agriculture, Regions and Tourism

SPONSORS

HUAWEI

T3K.AI

EXHIBITORS

Digital Factory Vorarlberg FH Vorarlberg University of Applied Sciences

T3K.AI

MEDIA

COMPUTERWELT

ACKNOWLEDGEMENTS

Thanks to our partners for their tremendous support

REWATCH IDSF2020

All keynotes, presentations, images and tech demonstrations are accessible online at idsf.io

ANNOUNCEMENT IDSF22

See you at IDSF in early 2022!
Sign up for our newsletter, we keep you posted: www.idsf.io

#IDSF22

THE IDSF ORGANISATION TEAM

Helmut Leopold
IDSF Initiator, Head of Center for Digital Safety & Security at the AIT Austrian Institute of Technology

Michael Mürling
Head of Event Organisation, Marketing and Communications Manager at the AIT Austrian Institute of Technology

Matthias Grabner
ADVANTAGE AUSTRIA / WKÖ AUSSENWIRTSCHAFT AUSTRIA / go-international

Wolfgang Grabuschnig, Donald Dudenhoeffer
Conference Programme

Verena Serini, Philipe Reinisch
Exhibition and Sponsorship

Contact
Please visit the conference website regularly for new information about this conference at idsf.io or send an email to idsf@ait.ac.at

Editorial Team
Helmut Leopold, Wolfgang Grabuschnig, Michael Mürling, Ross King, Andreas Kriechbaum-Zabini, Bernhard Strobl, Bernhard Haslhofer, Willibald Krenn, Georg Neubauer, Donald Dudenhoeffer

Location Images
Valerie Maltseva / Agenda Studio

Design
WHY. Studio

INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

www.idsf.io