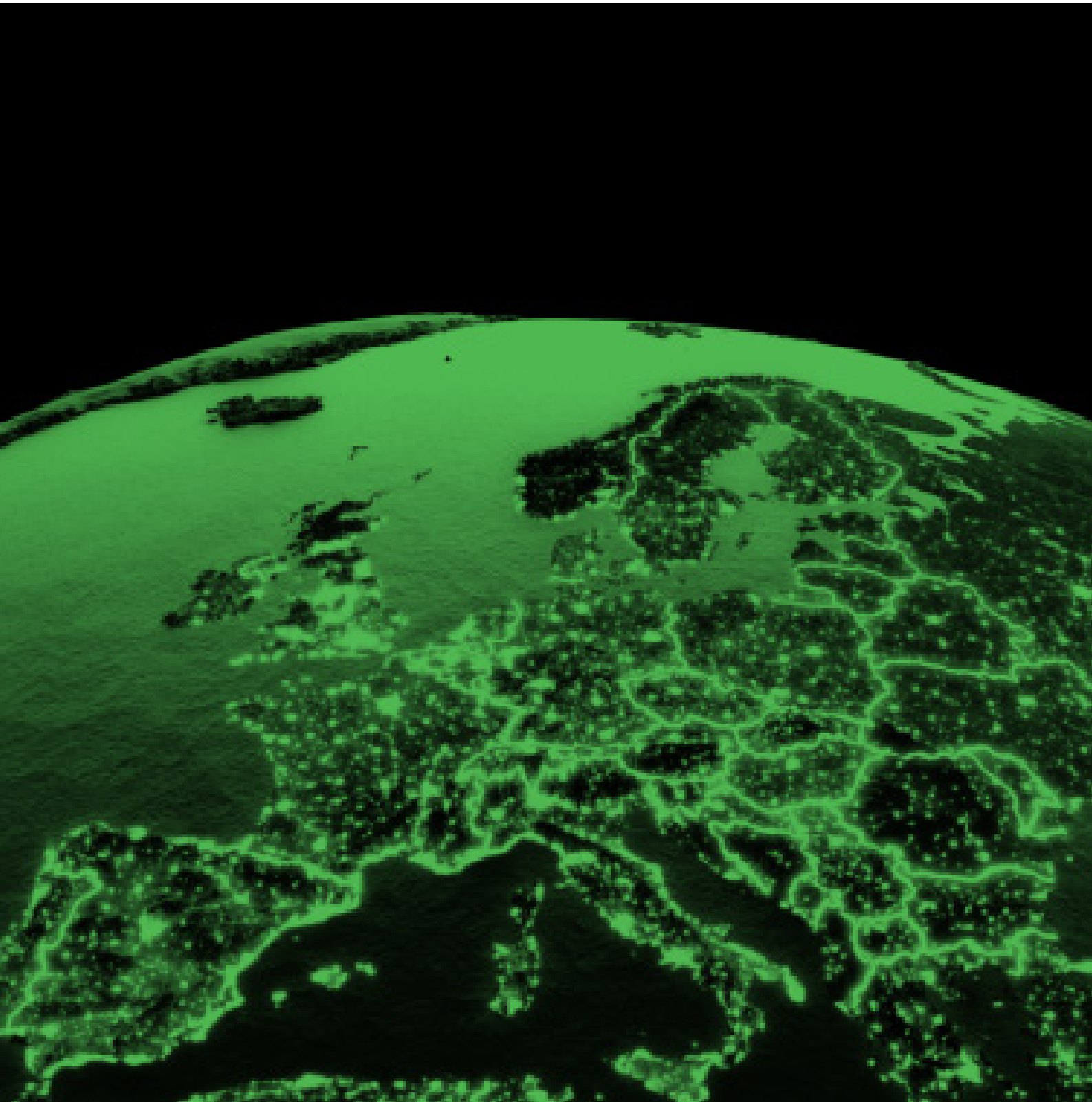
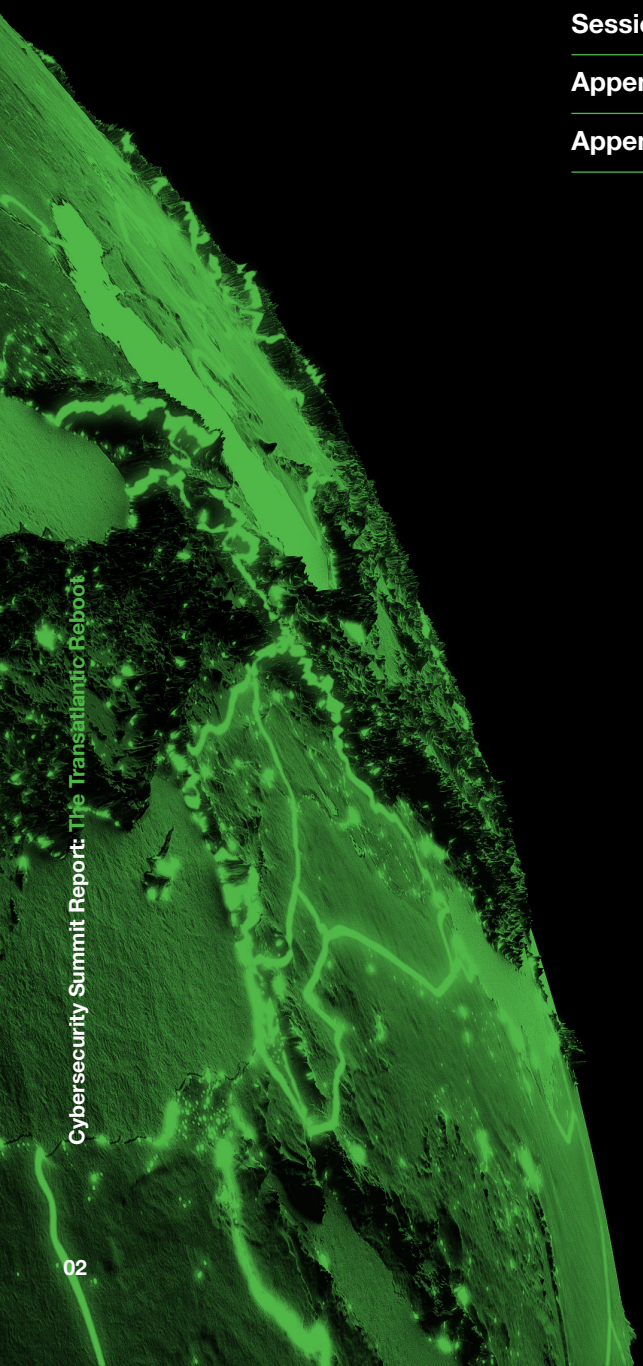
Ibec Global

Cybersecurity Summit Report: The Transatlantic Reboot



Contents

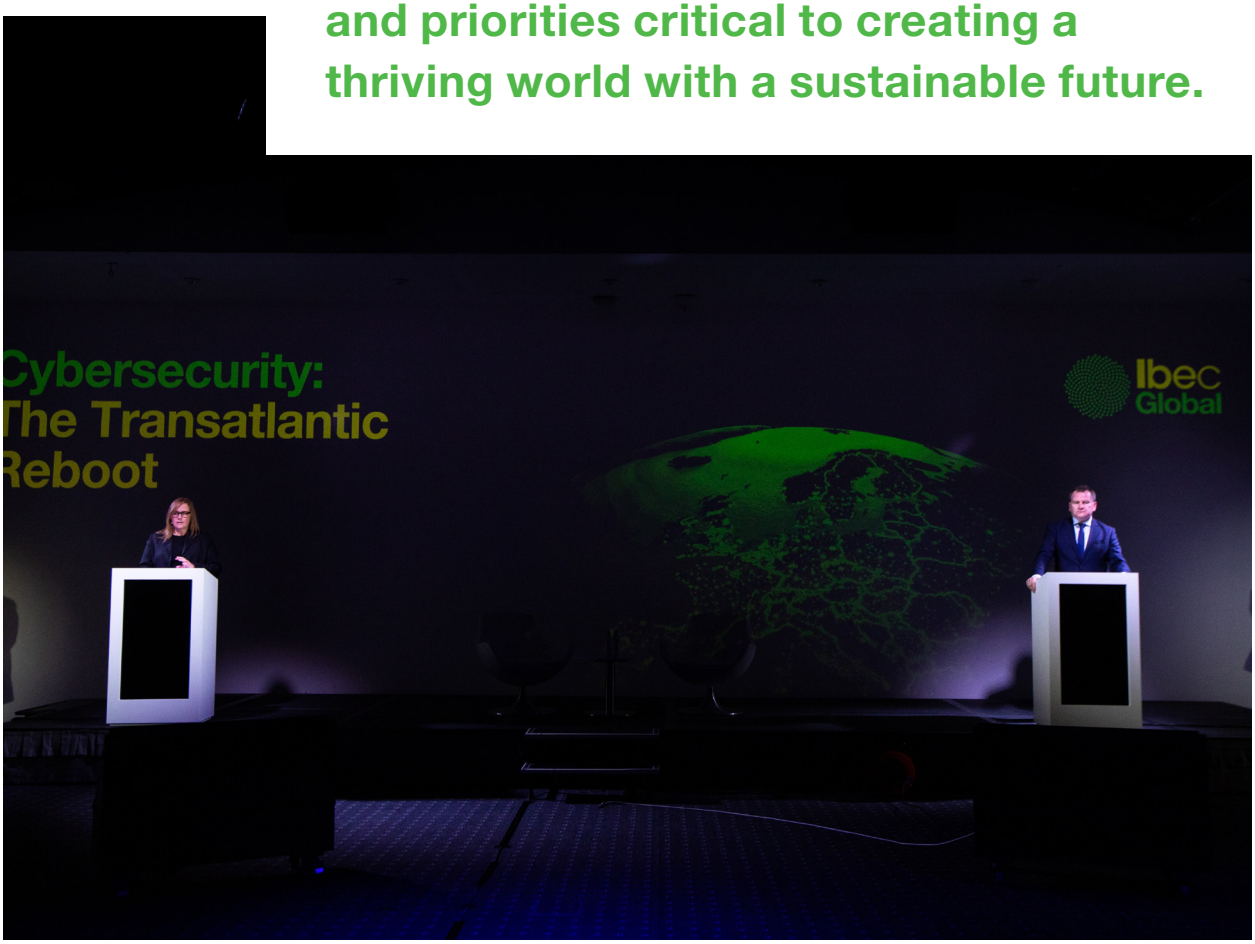


About Ibec Global

Ibec Global is the International Business Division of Ibec - Ireland's largest and most influential business representative organisation. We are Europe's standout anglophone business network globally and expert on the shifting relationships between the EU and the UK. We are a promoter of the EU single market and specifically interested in its ever-evolving relationship with the rest of the world, in particular its major trading partners including North America and the UK.

Pictured below:
Jackie King, Executive Director, International Business, Ibec; Danny McCoy, CEO, Ibec.

Our purpose is to convene key international stakeholders and decision makers to debate and shape the trends and priorities critical to creating a thriving world with a sustainable future.



Our work focuses on identifying and harnessing the international business trends and opportunities that fuel growth for businesses; advocating for enlightened policies and models in the context of major societal, policy, geopolitical and business trends; and influencing the conditions and providing the support for businesses to thrive globally.

In 2022, we will achieve this through three inter-connected workstreams:

1. Insights and analysis.
2. High-level engagement and facilitation.
3. Business community discourse, education and services.

Introduction

By Professor Ciaran Martin CB, Professor of Practice, Blavatnik School of Government, Oxford University and founding Chief Executive, National Cyber Security Centre (UK).

For more than a decade it has been a cliché to describe how we are becoming ever more dependent on digital technology. But all good clichés are based on a kernel of truth, and sometimes, over time, the truth becomes glaringly obvious. And during the pandemic, our relationship with technology changed from one of predicted dependence to one of actual dependence.

For many of us, technology allowed us to stay professionally just about afloat, and personally, just about OK. It allowed us to keep businesses and services going, and to keep in touch with loved ones we weren't allowed to see in ways never done before. Had our technology infrastructure not coped with the surge in demand, or had there been a catastrophic series of security failures, 2020 and 2021 would have been even worse than they already were. Those who kept our technology going – the engineers who did late night repairs to restore connectivity to isolated areas for example – are among the heroes of the great crisis of our time.

But as we move out of the pandemic, we must realise that if our relationship with technology has changed, then our thinking about it surely needs to change too. The security of our digital homeland is now a public good, so we need to act like it is one. For years, the debate around our cyber security has been shaped by national security strategists. One understandable consequence of that is that our language and attitude towards the cyber realm is often characterised in quite militarised language: cyberspace is, according to NATO since 2016, a "domain of operations". And cyberspace is indeed a domain of military operations. But is it primarily one?

I think it is much better to think about cyberspace as an artificially created environment where millions of us go to live and work. And if we think about it as an environment, then the two great challenges of our time in securing that environment become easier to think about.

The first challenge is the inherent insecurity of the Internet we have built. In the words of Dr. Vinton Cerf, one of the 'godfathers' of the Internet and architect of many of Google's technological breakthroughs, when the communications revolution was beginning, "we didn't think enough about those who would try to break the system". The understandable and necessary emphasis on connectivity above all else has bequeathed us a patchwork of difficult and serious vulnerabilities. Think of all the well know cyber attacks: a vulnerability unpatched; easy to exploit hardware; security measures that aren't easy to follow or implement. These are environmental factors. And these can be and are exploited by the pollutant of malicious code.

A second challenge is the rise of a different type of digital environment. A large number of Western security officials claim to have authored the revealing phrase that when it comes to digital security, Russia is severe bad weather, but China is climate change. That so many claim ownership signifies there is something in it. For a quarter of a century we have assumed that for all its faults, the West's version of a free and open Internet is the only possible one. No longer; the world is moving towards two 'technospheres' where one is liberal and one is authoritarian. Making sure free and open technology not just survives but flourishes is a century defining challenge.

But as technology changes we have a chance to address both problems. Those who built the technology we depend upon could not have foreseen these challenges. But we can now see the path ahead. We have to make our online world safer, more secure and more trustworthy whilst keeping it free and open. But we have the tools to do so. We now need the will to focus on the tasks. In time, demands for safer software and safer hardware will be seen in the same way as our current expectations of safer public transport and safer drinking water. And if we work together to protect our digital environment, we will protect all our futures.

Summit Executive Summary

18th November 2021

It was in this context that Ibec Global convened international experts, decision makers and thought leaders from government, security, academia, and business from both sides of the Atlantic to advance international cooperation, and a multi-stakeholder approach to cybersecurity to better protect critical infrastructure, citizens and businesses. The hybrid event was hosted from Brussels and included some 20 international leaders, experts and academics in cybersecurity from business, government, law enforcement, international alliances, national and international organisations and leading research centres and universities. (See Appendix A for a complete list of speakers).

Through keynotes and panel discussions, speakers covered the following themes (See Appendix B for the Summit agenda):

- **Deepening international cooperation and building trust.**
- **Advancing multi-stakeholder, international cooperation.**
- **Cybersecurity is a business issue - corporate risk and resilience.**
- **Global case study: HSE Ransomware Attack - Major attack on a critical state infrastructure, lessons for corporates and state agencies.**
- **Effective multilateralism and cybersecurity standard setting.**
- **State and industry partnerships.**
- **Cleaning up the cybersphere and what lies ahead.**

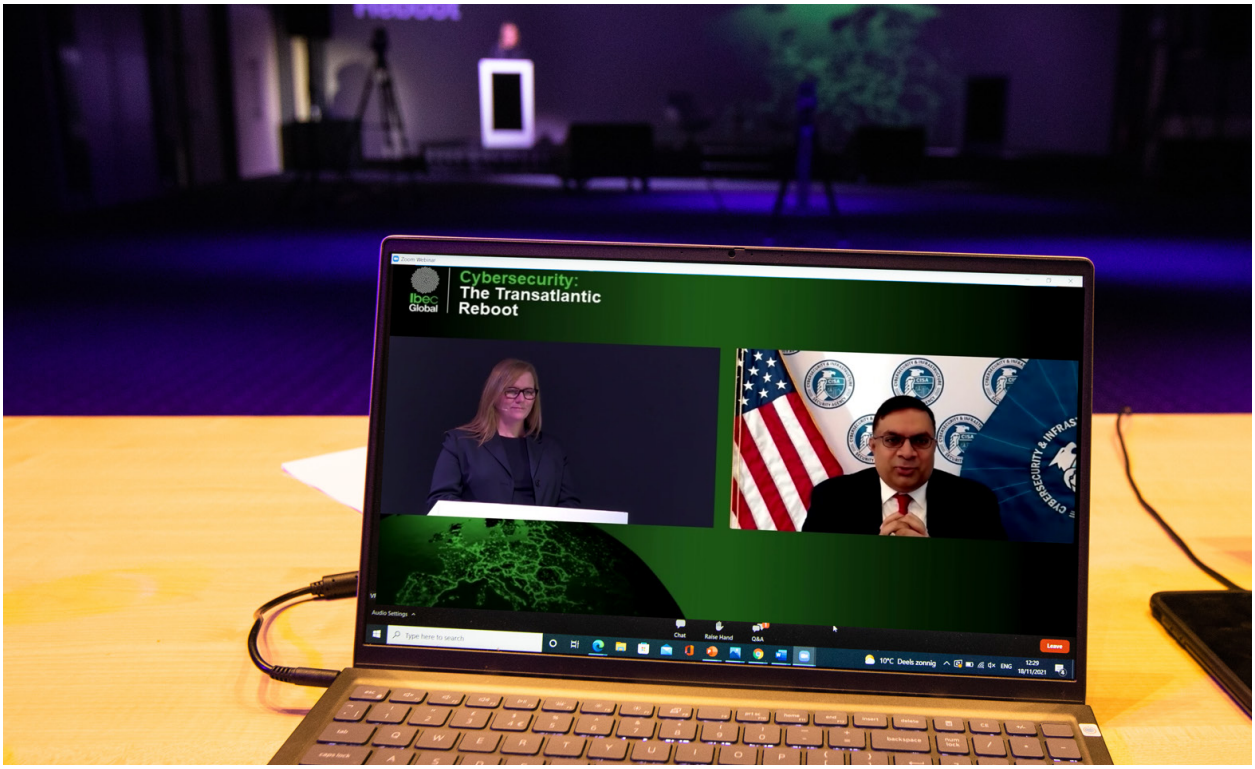
The key findings and calls to action that emerged from the Summit included the urgent need for major advanced economies to strengthen their cooperation to build robust resilience in cybersecurity to protect and defend their economies and societies, and the need to build much greater awareness to the damage of cyber attacks.

Many of the global expert speakers and panellists said repeatedly and emphatically that time is of the essence and we can procrastinate no more, because we have already seen the devastating effects and impacts of not working closely and better together. Only a genuinely international, multi-stakeholder collaborative approach can tackle what is an international threat.

Collaboration between public and private sectors was emphasised, with a number of speakers praising previous collaboration between the sectors at critical moments, including after Ireland's HSE ransomware attack.

Increased cyber resilience was also a common thread, with several speakers calling for enhanced cybersecurity resilience measures to be implemented as a matter of urgency. These include basic cybersecurity attack management plans, improved basic cyber hygiene and early detection systems.

Pictured below:
Jackie King, Executive Director, International Business, Ibec and Nitin Natarajan, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA).



The impact of the COVID-19 pandemic on global society and on cybersecurity has been profound, especially in the wake of the 2021 Cyber Attack on Health Services Executive agency of the Government of Ireland - a major ransomware attack on a critical infrastructure. It has been warned that these attacks may become more common, as criminals attempt to undermine crucial services such as health, energy and transport.

A number of speakers called for improved cybersecurity measures from legislators at a European and international level to address increasing security threats posed by malicious actors, as well as countries such as Russia and China. Increased funding to promote innovation and security and to tackle the skill shortage in the cyber sector was also called for, as it was revealed that there are huge personnel and skill shortages in the sector. Both the U.S. and EU have pledged to strengthen cybersecurity and collaborate to improve the cybersphere following the election of the Biden-Harris Administration. The EU is implementing a new cybersecurity competency centre in Romania, while NATO is initiating a new innovation lab to combat cyber threats.

International collaboration and cooperation between national cybersecurity teams can ensure that we are best prepared for any potential cyber attack, and by working together we can minimise the risk and potential damage we may face.

Pictured above:
Mircea Geoană, NATO Deputy Secretary General.

Session Highlights

Keynote

Deepening International Cooperation and Building Trust

Delivered by
Mircea Geoană,
NATO Deputy Secretary General.

The conference opened with a keynote speech from Mircea Geoană. He spoke about the impact of modern technology on business, economies and our way of life, warning of the 'real danger' of taking technologies for granted.

He spoke of how NATO has established a €1 billion Innovation fund to support and attract public and private investment to enhance cyber resilience. "My job is to drive forward innovation", said Mr. Geoană.

The NATO DSG emphasised the need for events such as the conference to bring together like-minded people, who share the same commitments in progressing cyber security.

He cautioned that super-powers such as Russia and China have made significant progress in their cyber capabilities and were attempting to interfere with Western society and democracy.

Mr. Geoană explained that 80% of innovation in cyber and technology is currently undertaken by the private sector, meaning private-led technology can pave the way for universal technologies available to everyone.

The NATO Deputy Secretary General stressed the importance of fostering innovation in society, while upholding fundamental rules of democracy, free speech and rule of law. Mr. Geoană called for cyber stability and a free and open cyberspace for the world to share. He said "cyber and new technology must be for all, shared by all and must work for all".

Key Takeouts:

- **We cannot take technological advantages for granted.**
- **We need to promote cyber stability with free open secure cyber spaces.**
- **Cyber and new technology must be for all, shared by all and must work for all.**
- **We need to build early detection systems, and build a network across the EU.**
- **It's important for the 27 EU Member States to work with global partners.**
- **We need deterrents, laws, justice and sanctions to prevent cybercrime.**
- **We have made a step in the right direction but we need to move more and work as common actors to tackle this issue.**

Panel Discussion 1:

Advancing Multi-Stakeholder, International Cooperation

Despina Spanou	Head of Cabinet for European Commission Vice President Margaritis Schinas
Craig Jones	Director of Cybercrime, INTERPOL
Ossian Smyth TD	Minister of State with Responsibility for Public Procurement and eGovernment; Communications and Circular Economy, Ireland
Sami Khoury	Head of the Canadian Centre for Cyber Security

Panel Discussion 1

Despina Spanou

Head of Cabinet of European Commission Vice President Margaritis Schinas

The Summit heard from Despina Spanou, the Head of Cabinet for Commission Vice-President Margaritis Schinas. Ms. Spanou emphasised the requirement for urgent global collaboration on cybersecurity. She stressed that the EU needs to collaborate with global partners to develop deterrents, laws, justice and sanctions to tackle cybercrime.

Ms. Spanou described how COVID-19 has exacerbated cybersecurity issues faced by countries, with criminals now targeting critical infrastructures such as hospitals to wreak havoc across society.

The Commission official recommended that we switch to an 'operational aspect' to combat cyber threats, revealing that the European Union Agency for Cybersecurity (ENISA) identified ransomware as the prime threat in 2021.

She advocated for improved early detection systems and a cross-border network across the EU to finance collective knowledge targeted to fighting cybercrime. She also described how the EU would be establishing a new cyber competency centre in Bucharest, which will bring together public and private stakeholders.

Ms. Spanou announced the establishment of the Europol Innovation Lab, with officials from the public and private sector tasked with fighting cybercrime. Ms. Spanou concluded by calling for greater collaboration between the U.S. and Europe to counter cyber threats.

Key Takeouts:

- **We need to build early detection systems, and build a network across the EU.**
- **It's important for the 27 EU Member States to work with global partners.**
- **We need deterrents, laws, justice and sanctions to prevent cybercrime.**
- **There is clear momentum on both sides of the Atlantic with EU and US relations on this matter.**
- **We need to build resilience through an operational approach.**

Panel Discussion 1

Craig Jones

Director of Cybercrime, INTERPOL

The Director of Cybercrime with INTERPOL joined the Summit by live link from Singapore. Mr. Jones spoke about INTERPOL's role in connecting policing organisations across the world. He emphasised there was still a long way to go to tackle cybercrime and called for a more operational and regulated model to share information across borders.

He stressed the importance of working with private sector partners to combat cyber and ransomware threats and highlighted the need for regional information hubs to share critical data.

Key Takeouts:

- **Cyber criminals take advantage of vulnerabilities to commit their crimes.**
- **We need a more operational approach and loop together and trust each other to share information.**

Panel Discussion 1

Ossian Smyth TD

Minister of State with responsibility for Public Procurement and eGovernment; Communications and Circular Economy, Ireland

Ireland's cyber Minister Ossian Smyth spoke from Government Buildings in Dublin. Mr. Smyth said there was a need for greater cyber diplomacy and increased coordination of cyber policies to tackle cyber threats. He emphasised that collaboration is 'essential' to combating these potential threats, as well as being more open about sharing information on a global scale.

Mr. Smyth spoke about the EU's plans to enhance cyber resilience through the NIS2 Directive on security of network and information systems and underscored the need to share information with trusted parties.

Minister Smyth also highlighted the importance of investment in the cyber sector, to foster innovation and job creation in the sector. He stressed that there is also great potential to expand cyber security operations in Europe and enhance international collaboration in the sector.

Key Takeouts:

- **International collaboration is essential.**
- **Cooperation needs to be beyond EU borders.**
- **The EU needs to maintain an outward global focus.**

Panel Discussion 1

Sami Khoury

Head of the Canadian Center for Cyber Security

The Head of the Canadian Center for Cyber Security, Sami Khoury, spoke of the importance of global partnerships at a strategic level to fight cybercrime, promising that it will help "make tomorrow better than today". He warned that cybersecurity is the most likely threat to impact us in the years ahead.

Maintaining a safe cybersecurity system requires investment over time and requires a collective approach. New models of shared communications are critical, with cyber resilience likened to the ability to anticipate, withstand, and recover from a cyber attack.

Key Takeouts:

- **Partnership is critical. Our role is to help make tomorrow better than today.**
- **A better tomorrow means better cybersecurity.**
- **We cannot do this alone. Cybersecurity is a team sport and we must each play our part.**
- **We need to work together and force a shift. Forums and discussions like these are critical, and we can be better positioned to respond to threats.**

Keynote

View from Europe

Delivered by
Lorena Boix Alonso,
Digital Society, Trust and Cybersecurity, DG CONNECT.

The Head of the Cybersecurity Unit at the European Commission's DG CONNECT, Lorena Boix Alonso emphasised not nearly enough was being done quickly enough to tackle international scourge of cybercrime.

Ms. Boix Alonso said that while the world has previously identified these cybersecurity threats as a 'wake up call', they need to be taken seriously. Ms. Boix Alonso called for increased collaboration by officials on both sides of the Atlantic, and said the U.S. and EU were determined to work together to improve the cybersphere.

She stressed that we need to improve our operational capacity by advancing a global and open cyberspace through increased cooperation. She added we need a 'robust system' of detection, strategy, and enforcement.

Ms. Boix Alonso revealed new initiatives under the European Cyber Resilience Act that will set common security standards on devices in the European Market. To achieve this, working with the U.S. is essential.

Key Takeouts:

- **Working with the United States is absolutely essential.**
- **We have all witnessed cyber security incidents as 'wake up calls', which show we are not doing enough or not moving fast enough. These wake-up calls need to be taken seriously.**

Keynote

View from the U.S.

Delivered by
Nitin Natarajan,
Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security.

Joining the Summit on a live link from Washington D.C., Mr. Natarajan spoke about the shared digital threats experienced by the U.S. and EU, calling for increased cooperation between the two to tackle cybercrime.

He stressed that we are "stronger together" before and after a cyber attack by sharing information with each other and called for bold action in the sector.

Mr. Natarajan warned against emerging hybrid threats in the sector and called for collaborative risk management to mitigate these risks. Following on from Ms. Boix Alonso's statement, Mr. Natarajan also called for improved security measures on network devices.

He emphasised the importance of collaboration between U.S. and European officials in cyber to 'shape global policy' and set international norms.

Key Takeouts:

- **If we have a collective defence, we are stronger together, before, during and after a cyber attack by sharing information.**
- **We need to take bold action.**
- **We need to prioritise the top risks, and provide services to combat risks, as well as building capacity and driving change.**
- **Cyber is now a battlefield and we need a common strategy.**
- **We can't prevent everything, and everyone needs to do their part with basic cyber hygiene systems and involve the private sector.**

Keynote

Cybersecurity is a Business Issue

Delivered by
Robert Booker,
Senior Vice President
& Chief Information
Security Officer Emeritus,
UnitedHealth Group.

The view of the industry and the private sector was represented by Robert Booker, UnitedHealth Group's CISO. Mr. Booker spoke about cybersecurity threats to consumers and patients of a commercial health group.

He emphasised the need for business leaders to educate themselves on cyber threats, protection systems and operational risk. He called for broader collaboration between private companies and industry and transparency for stakeholders.

He warned that a lack of security "leads to a lack of trust".

Key Takeouts:

- **Healthcare and cybersecurity is a global imperative.**
- **Cyber threats continue to evolve and have a clear impact, and have an increasing downstream effect.**
- **A lack of security leads to a lack of trust.**

Panel Discussion 2:

Corporate Risk and Resilience

Rois Ni Thuama PhD Head of Cyber Governance, Red Sift

EJ Wise Principal, Wise Law Cyber Consulting

Clare Barnett Director, Invest City of Brampton (Ontario, Canada)

Remarks were followed by panel discussion moderated by: Danny McCoy, CEO, Ibec.

Panel Discussion 2

Rois Ni Thuama PhD

Head of Cyber Governance, Red Sift

Speaking about the ENISA '2021 Threat Landscape' report, Ms. Ni Thuama identified the three prime threats facing the cybersphere today. These include ransomware, malware and email threats.

Despite increasing innovation and cyber attacks, these threats remain predominantly the same as threats identified in the nine previous reports, which identify ransomware, malware, scareware, worms and trojans as potential threats.

She emphasised that the story remains the same, but the actors change. She stressed that the problems we face are chronic rather than catastrophic, and with reasonable care, skill and diligence we can handle these threats.

She highlighted the importance of taking cyber threats seriously, as an attack can do undue damage to a company's reputation and share price. Ms. Ni Thuama called for the implementation of basic cyber hygiene and cyber resilience to bolster our defences.

Key Takeouts:

- **The story is the same, but actors change.**
- **Problems we face are chronic and are not catastrophic.**

Panel Discussion 2

EJ Wise

Principal, Wise Law Cyber Consulting

The importance of proper legal and insurance risk analysis was raised by Squadron leader, EJ Wise. Ms. Wise called for society to adapt our thinking and implement incident response plan and cyber attack response plan, as standard.

She called for companies to immediately establish an incident response plan, and demand they know what to do in the event of a cyber attack.

Ms. Wise spoke about the potential of 'hacking-back' but cautioned, as she was unsure of the legalities surrounding the practice. She warned that it was similar to paying ransom to criminals.

Key Takeouts:

- **Every time we pay ransoms, we fund further crime.**

Clare Barnett

Director, Economic Development, City of Brampton

The City of Brampton is an innovation district in Canada and is in the heart of Canada's innovation corridor. Ms. Barnett spoke about the city's development as an innovation hub, training facilities and opportunities for workers.

She called for increased investment in cyber security, as well as support for start-up companies and cybersecurity organisations.

Key Takeouts:

- **We need a strategic approach with new technologies, ecosystems and investment in cybersecurity.**

HSE Ransomware Attack: The First Major Attack on a Critical State Infrastructure, Lessons for Corporates and State Agencies

Global Case Study

Fran Thompson

Chief Information Officer, HSE

The biggest cyber attack known to take place against a national health service was on Ireland's Health Service Executive in May 2021.

Chief Information Officer at Ireland's Health Service Executive, Mr. Thompson was at the cold face.

Mr. Thompson described how the significant malicious ransomware infected the HSE's infrastructure, impacting 80% of the HSE's systems. He told the conference that the HSE is currently in its final recovery and learning phase post-attack.

A key takeout from the attack was that cybersecurity and governance are a leadership issue, and not just solely IT. Mr. Thompson called for organisation leaders to be aware of how their businesses are dependent on technology, and what to do if this technology fails.

He advised organisations to carry out simulated attacks to prepare for potential threats and stressed the need for companies to have a cybersecurity strategy in place, cyber specific crisis management plan and cybersecurity incident response plan, as well as a business continuity plan for a cyberattack.

Key Takeouts:

- **Prevention is far better than a cyber attack.**
- **Sharing of information at the right time is so important.**
- **Organisations must have a cybersecurity strategy and leadership.**
- **Cyber is not just an ICT issue, it's a business issue.**

Global Case Study

Detective Chief Supt. Paul Cleary

Garda National CyberCrime Bureau

The Head of Ireland's National CyberCrime Bureau joined the Summit via video link from Dublin, where he revealed that the criminal investigation into the HSE attack was still active.

Det. Chief Supt. Cleary also said that the body would be planning a number of operations over the coming months into the attack. He revealed that evidence from nine jurisdictions around the world had been retrieved.

International policing partners and Ireland's police force had targeted and seized suspect technical infrastructure, including domains used by the criminals. This action allowed the authorities to alert other potential victims, preventing attacks on 753 victims around the world.

Disrupting criminal finances was becoming more challenging, as criminals adapted to new cryptocurrencies such as Monero. The HSE cyber attack had been an eye-opener to the CyberCrime Unit and international partners in Interpol and Europol.

Det. Chief Supt Cleary advised that cyber should be treated as an investment, rather than an overhead by organisations, if they are serious about tackling cybercrime and wading off any potential cyber attacks.

Key Takeouts:

- **The only way to defeat cyber attacks is collaboration and cooperation.**
- **We need to keep the pressure on cyber criminals.**
- **Organisations must have a plan, preparedness and must be aware of the risks.**
- **We have to treat cybersecurity as an investment rather than an overhead.**

Keynote

Cleaning up the Cybersphere & What Lies Ahead

Delivered by
Professor Ciaran Martin CB, Professor of Practice, Blavatnik School of Government, Oxford University and founding Chief Executive, National Cyber Security Centre (UK).

Professor Ciaran Martin CB reminded attendees that cyberspace should be treated as a geopolitical issue, owing to the fact it is an artificially created environment. However, he believes the issue with the internet is that it is structurally insecure.

Upon its inception, the internet was private-sector driven and emphasised connectivity and networking without security in mind.

Professor Martin highlighted previous cyber attacks, such as the Talk Talk attack in 2014 and most recent HSE attack, as examples of the fragility of the digital environment.

He echoed Det. Chief. Supt. Cleary's comments on the difficulty of criminal jurisdictions but advocated for basic cyber hygiene and building resilience in our current cyber capabilities.

Key Takeouts:

- **We need to build cyber resilience.**
- **It's always in our interest to secure the cyber environment.**
- **We need to do the basics well, by building resilience, educating leaders and as citizens demanding better security.**

Panel Discussion 3:

International Cooperation on Norms and Standards

Stephen Rae	Publisher, AML Intelligence and Principal, KOBN
Cristian Silviu Buşoi	MEP, Chair of Parliament Committee on Industry, Research and Energy
Dr. Richard Browne	Director, National Cyber Security Centre
Kathleen Moriarty	CTO, Center for Internet Security
Merle Maigre	Senior Cyber Security Expert, e-Governance Academy, Estonia

Panel Discussion 3

Cristian Silviu Buşoi

MEP, Chair of Parliament Committee on Industry, Research and Energy

The Chair of the European Parliament's Committee on Industry, Research and Energy and MEP, Cristian Silviu Buşoi emphasised the importance of cybersecurity for the EU, adding that we need to coordinate our efforts to tackle emerging cyber threats.

The increasing number of devices in our system will result in a rise in cyber attacks, warned Buşoi, who advocates for a 'preventative approach' to cybersecurity.

The MEP called for increased information sharing to ensure an "open, free and secure cyberspace". He also called for the European Commission to take decisive action to protect security in the bloc.

ENISA will soon establish a new EU cyber technology and research competency centre in Romania that will be tasked with coordinating research in cybersecurity in the EU.

Key Takeouts:

- **We need to act together and collaborate on an international level.**
- **We need to work together and use cyber diplomacy, and have more integrated and coordinated policies.**

Dr. Richard Browne

Director, National Cyber Security Centre (Ireland)

The scope of the internet was discussed by Dr. Richard Browne, who stressed that improved cyber resilience would allow internet users to be better protected and informed.

He advocates for enhanced standards and security for all users and spoke about cyber security on a national level and its links to the public sector.

Key Takeouts:

- **The internet is a global system of global norms which poses a series of different challenges. How do we refrain and reshape?**

Panel Discussion 3

Kathleen Moriarty

CTO, Center for Internet Security

Like Professor Ciaran Martin, Ms. Moriarty emphasised that the internet was not built securely. She revealed that the cyber industry currently has a $3.5 million security professional deficit worldwide.

She stressed we need to embrace enhanced security controls and measures to improve our cyber sphere.

Key Takeouts:

- **We need to embrace and push security controls to the endpoint.**

Merle Maigre

Senior Cyber Security Expert, e-Governance Academy

A Senior Cyber Security Expert at the e-Governance Academy in Estonia, Ms. Maigre called for citizens to uphold fundamental freedoms through the cyber sphere and called for a 'common baseline' to be built on the European NIS2 Directive.

Key Takeouts:

- **Our role is to uphold fundamental freedoms and protect individuals from unlawful citizens.**

Appendix A

Speakers List

Mircea Geoană	NATO Deputy Secretary General
Lorena Boix Alonso	Director for Digital Society, Trust and Cybersecurity, Directorate General for Communications Networks Content and Technology (DG CONNECT)
Craig Jones	Director of Cybercrime, INTERPOL
Nitin Natarajan,	Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security
Robert Booker	Senior Vice President & Chief Information Security Officer Emeritus, UnitedHealth Group
Despina Spanou	Head of Cabinet for European Commission Vice President Margaritis Schinas
Ossian Smyth TD	Minister of State with Responsibility for Public Procurement and eGovernment; Communications and Circular Economy, Ireland
Cristian Silviu Buşoi MEP	Chair of Parliament Committee on Industry, Research and Energy
Sami Khoury	Head of the Canadian Center for Cyber Security
Clare Barnett	Director, Economic Development, City of Brampton
Dr. Richard Browne	Director, National Cyber Security Centre (Ireland)
Detective Chief Supt. Paul Cleary	Garda National CyberCrime Bureau
Paul de Souza	President, Cyber Security Forum Initiative (CSFI)
Merle Maigre	Senior Cyber Security Expert, e-Governance Academy
Kathleen Moriarty	CTO, Center for Internet Security
Fran Thompson	Chief Information Officer, HSE
Dan Cimpean	Acting Director, Romanian National Cyber Security Directorate
Professor Ciaran Martin CB	Professor of Practice, Blavatnik School of Government, Oxford University and founding Chief Executive, National Cyber Security Centre (UK).
EJ Wise	Principal, Wise Law Cyber Consulting
Rois Ni Thuama PhD	Head of Cyber Governance, Red Sift

Appendix B

Opening Remarks
Delivered by Jackie King, Executive Director, International Business, Ibec.

Opening Address – View from Europe
Delivered by Lorena Boix Alonso, Digital Society, Trust and Cybersecurity, DG CONNECT.

Keynote – Deepening International Cooperation and Building Trust
Delivered by Mircea Geoană, Deputy Secretary General, NATO.

Discussion – Advancing Mutli-Stakeholder, International Cooperation
Panel:
Despina Spanou, Head of Cabinet of European Commission Vice President Margaritis Schinas.
Craig Jones, Director of Cybercrime, INTERPOL.
Ossian Smyth TD, Minister of State, Public Procurement and eGovernment, Ireland.
Sami Khoury, Head of the Canadian Centre for Cyber Security.
Speaker remarks were followed by a moderated Q&A.

Keynote – View from the U.S.
Delivered by Nitin Natarajan, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security.

Keynote – Cybersecurity is a Business Issue
Delivered by Robert Booker, Senior Vice President & Chief Information Security Officer Emeritus, UnitedHealth Group.
Followed by one-on-one with Danny McCoy, CEO, Ibec.

Discussion – Corporate Risk and Resilience
Panel:
Rois Ní Thuama PhD, Head of Cyber Governance, Red Sift.
EJ Wise, Prinicpal, Wise Law Cyber Consulting.
Clare Barnett, Director, Economic Development, City of Brampton (Ontario, Canada).
Remarks were followed by a panel discussion moderated by: Danny McCoy, CEO, Ibec.

Global Case Study - HSE Ransomware Attack: The First Major Attack on a Critical State Infrastructure, Lesson for Corporates and State Agencies
Fran Thompson, Chief Information Officer, HSE
Detective Chief Supt. Paul Cleary, Garda National CyberCrime Bureau.

Keynote – Cleaning up the Cyberspace and What Lies Ahead
Delivered by Professor Ciaran Martin CB, Professor of Practice, Blavatnik School of Government, Oxford University and founding Chief Executive, National Cyber Security Centre (UK).

Discussion – International Cooperation on Norms and Standards
Panel:
Cristian Silviu Buşoi, MEP, Chair of Parliament Committee on Industry, Research and Energy.
Dr. Richard Browne, Director, National Cyber Security Centre.
Kathleen Moriarty, CTO, Center for Internet Safety.
Merle Maigre, Senior Cyber Security Expert, e-Governance Academy, Estonia.
Remarks were followed by moderated panel discussion

Closing Keynote – State and Industry: We Are in This Fight Together
Delivered by Paul de Souza, President, Cyber Security Forum Initiative (CSFI).

If you would be interested in partnering with Ibec Global on our 2022 Cybersecurity Summit taking place in November, please reach out to us at **ibecglobal@ibec.ie**.

Dublin
Ibec Head Office
84/86 Lower Baggot Street,
Dublin 2 , D02 H720.
T: (01) 605 1500
E: membership@ibec.ie
W: ibec.ie/membership

Brussels
Ibec Global,
Avenue de Cortenbergh 89,
Box 2, B-1000 Brussels,
BELGIUM.
T: +32 (0)2 740 14 30
E: ibecglobal@ibec.ie

Ibec Global

Extend Ireland's global reach. Join the conversation.

@IbecGlobal

linkedin.com/company/ibecglobal

Ibec Global

www.ibec.ie/influencing-for-business/ibec-global