Protecting critical infrastructure against cyber threats

An analysis of relevant regulation, good practices, international law and norms

Summary Report of the Workshop Series
2022

Microsoft

EVRO-ATLANTSKI SVET SLOVENIJE
EURO-ATLANTIC COUNCIL OF SLOVENIA

REPUBLIC OF SLOVENIA
Government Information Security Office

URSIV

University of Ljubljana
Faculty of Social Sciences

Dear Reader

It is with great pleasure that we share with you this report titled 'Protecting Critical Infrastructure against cyber threats: An analysis of relevant regulation, good practices and international law'. The report summarizes the fruitful conversations held during the four workshops that took place in 2021, ahead of the Slovenian Presidency of the European Council. Their objectives were to understand ongoing cybersecurity threats, and identify good practices that could be implemented to raise the levels of cybersecurity across the world.

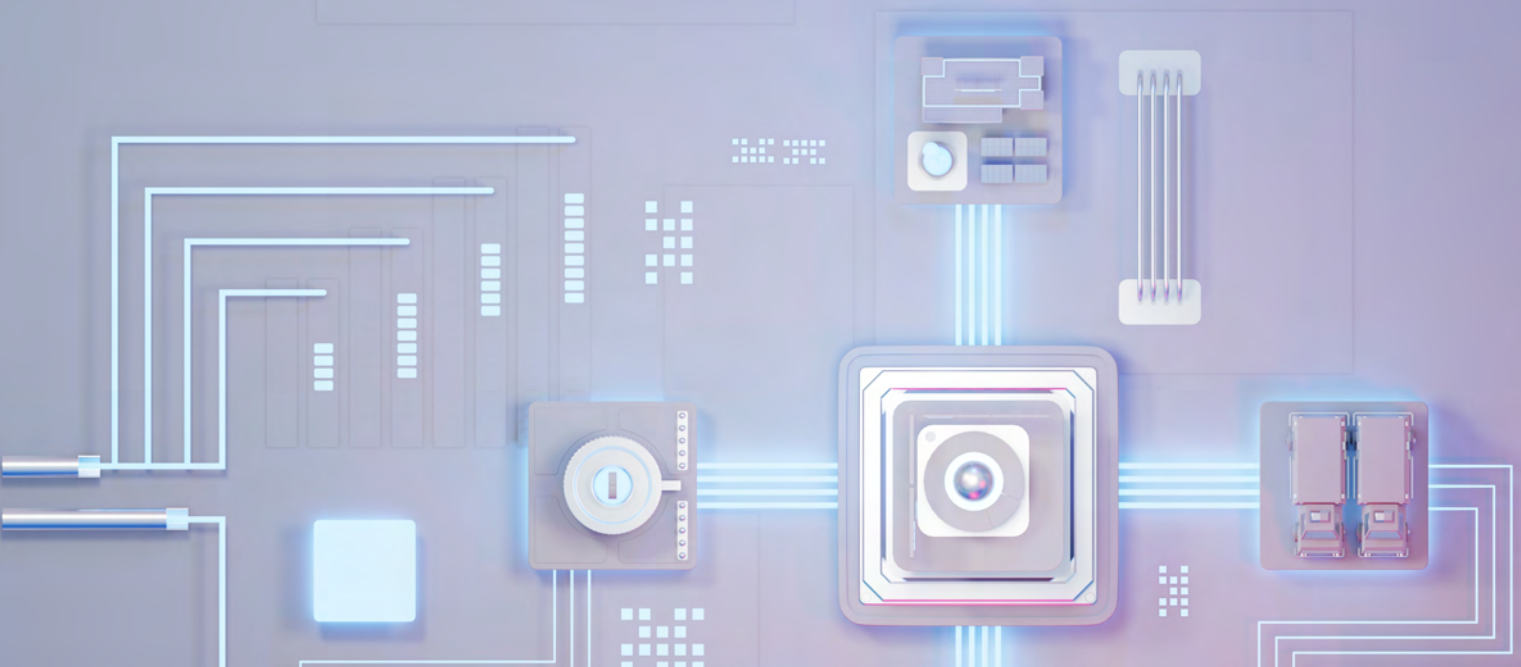
In the workshops participants examined four different critical infrastructure sectors: water, electric power, healthcare, and the financial sector. In each of the workshops attendees focused on cybersecurity threats that affect a particular sector, examined the current legislative and regulatory framework at the European Union (EU) and international levels, and then discussed potential recommendations to minimize the threats.

More than solely mapping out the challenges, the objective of the workshops was also to identify recommendations on how to improve the current state of play. It quickly became clear that cybersecurity cannot be treated as a one-off investment, but as a process. This includes continuous monitoring of the threat landscape, ongoing investments in the practices of individual organizations, continuous improvement of expertise through dedicated capacity building, and a frequent evaluation of the policy and regulatory frameworks. Another point that was repeatedly raised was the importance of communication between the different stakeholder groups, and the harmonization of approaches across borders, as the threats we face are not confined to particular countries.

The unique value of the series came from the diversity of participants, who attended from across the world, came from different disciplines, and provided varied perspectives on the potential paths forward. Through their participation we were able to identify trends and commonalities that we would otherwise not have seen, as well as better understand the linkages between technology, regulation, and international frameworks. We also hope that we were able to foster new connections that will feed into a continuous dialogue on this critical challenge. This was a real example of multistakeholderism in action and we want to thank all who participated!

This report seeks to faithfully capture the key points raised in the workshops and we hope that you find it as useful as we found the workshops.

Faculty of Social Sciences, University of Ljubljana
Government Information Security Office of the Republic of Slovenia
Microsoft
Euro-Atlantic Council of Slovenia



Contents

Introduction

Critical infrastructure and related essential services lie at the core of our societies. They increasingly rely on digital services to improve their operational efficiency and to bring services closer to citizens. However, online connectivity also exposes them to nefarious elements of cyberspace, including criminal and state actors. These can exploit, and have in the past exploited, cyberspace to cause mischief, collect intelligence, demand ransom, and purposefully destroy or disrupt services. When it comes to critical infrastructure, these attacks could result in a serious crisis or even lead to a kinetic conflict. As a result, both providers and users must rethink security features, protocols, and relevant regulations.

The Faculty of Social Sciences, University in Ljubljana, Government Information Security Office of the Republic of Slovenia, Euro-Atlantic Council of Slovenia, and Microsoft came together in the spring and summer of 2021 to examine the cyberthreats targeting critical infrastructure and to identify how to strengthen resilience. To this end, four webinars were organized between April and July 2021 to explore cybersecurity in the water sector (April 21), the electric power sector (May 12), the healthcare sector (June 2) and the financial sector (July 7). These were selected because of a series of cyberattacks that highlighted risks and vulnerabilities in these sectors. Since the workshops the number of attacks on these critical sectors have only multiplied.

Each of the workshops was organized around three sessions, focusing on:

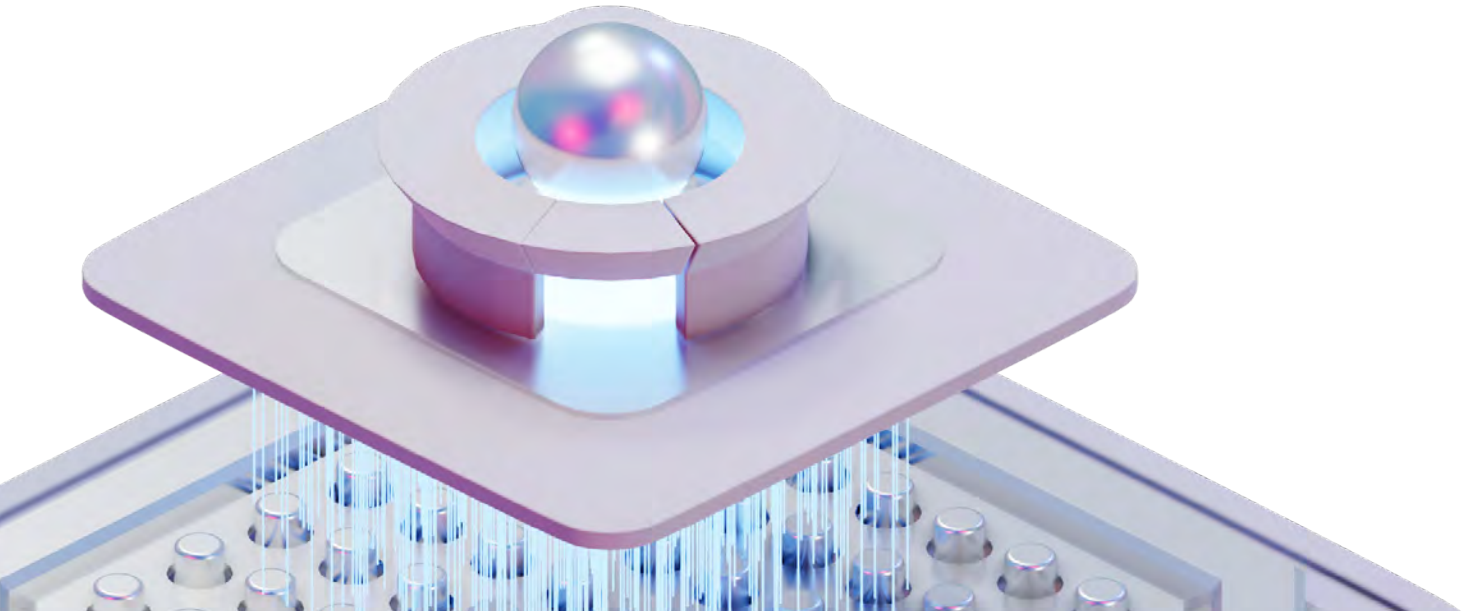
- **cyber threats and risks to the sectors,**
- **resilience and regulation, and**
- **the role of international law and norms.**

A common framework for all the discussions ensured that similar questions were posed across the different critical infrastructure sectors, allowing us to identify similarities and extrapolate recommendations that could be applicable more broadly.

For example, key concerns that emerged included:

- **increases in frequency and sophistication of cyberattacks, as well as the expanding attack surface;**
- **the potential for far reaching consequences of cyberattacks, given the interconnectedness of cyberspace;**
- **the lack of accountability for malicious actors, criminal or state-sponsored.**

This report goes beyond the concerns to reflect practical perspectives, findings, and lessons from the seminars. In the first part, we provide ten overarching recommendations, while the rest of the document contains numerous sector-specific lessons and good practices. The authors of this report sought to collect tangible outcomes and specific recommendations, but refrain from endorsing any of those in a particular manner.



Key Recommendations

1. **Cybersecurity must be understood as a continuous process.** There will always be important systems in need of protection against malicious actors with harmful intentions and sophisticated capabilities. Risk management needs to be at the heart of any approach we take.

2. **The cybersecurity field is still maturing. Technology continues to evolve, and attackers are innovating their techniques as well.** Cybersecurity is a rapidly adjusting field and it is likely to remain so for some time. We therefore need to continue working on good practices and improve regulatory frameworks consistently. While focusing on the outcome, we need to constantly assess the right path towards getting there.

3. **Harmonization of approaches is required.** Cyberattacks can have cross-sectoral effects. While we investigated individual critical infrastructure sectors, we recognize that not only do these often rely on the same technologies, but attacks against them can also spill over. Harmonization of good practices is required to ensure we do not do more harm than good with regulatory approaches.

4. **Information sharing is key.** Cybersecurity responsibilities are distributed among many regional, national, and industry actors. Often these entities do not talk outside their sector or country. However, attackers do not care for those boundaries, and we need increased information exchange as it relates to good practices, cyberattacks, and related defensive actions.

5. **Cybersecurity ecosystem must be based on trust.** CERTs, ISACs, and national competent authorities dealing with cybersecurity will likely have their responsibilities increase in the coming years. To ensure they are successful, creating an environment of collaboration, trust, and information exchange between public and private actors early on is key.

6. **Capacity building is required for further collaboration and trust building.** Our workshops echoed the call of the recent United Nations (UN) reports on cybersecurity—there is a clear cybersecurity skills gap and more capacity building is desperately needed.[1] The Global Forum on Cyber Expertise (GFCE)[2] and other platforms can play a critical role in further advancing these efforts, domestically and internationally.

7. **Existing international cybersecurity norms need to be implemented.** Governments in 2015 agreed on a set of international cybersecurity norms at the UN and these must be implemented.[3] Certain countries have already begun highlighting how they are approaching their commitment, but more work needs to be done.

8. **International law applies to cyberspace.** Recent discussions at the UN have made it clear that international law applies to cyberspace in its entirety.[4] Nevertheless, this is an emerging area of law and further work is needed to reach a common agreement as to how international law applies to cyberspace. National statements, as well as work at the European Union (EU) level, and examples of practical discussions, such as those under the Oxford Process can help clarify its applicability.[5]

9. **Attribution in cyberspace is a multidimensional tool that needs to be utilized.** Attribution has technical, political and legal dimensions. Our technical ability to attribute cyberattacks has improved, both in terms of accuracy and speed. Legal frameworks have also been strengthened. However, given the political dimension involved, attribution remains a sensitive act.

10. **There must be consequences for malicious actors.** Attacking critical institutions and services is still relatively risk free when compared to other criminal endeavors. Attackers are rarely identified and punished. This needs to change in both the domestic, and international contexts.

1 See Cybersecurity: https://unsceb.org/topics/cybersecurity.
2 See Strengthening cyber capacity and expertise globally through international collaboration: https://thegfce.org/.
3 See 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.
4 Ibidem.
5 See The Oxford Process: https://www.elac.ox.ac.uk/the-oxford-process/.

WORKSHOP 01

Water infrastructure and services

Summary of key take-aways for policymakers and practitioners

Cyberthreats and risks to the sector:

- **Criticality of the water management sector:** Water is a vital source of life, basic human need, and essential resource in various industrial activities. The water management sector is responsible for collecting, storing, cleaning, and providing water to people. Most of these activities are automated and facilitated by technology.
- **Vulnerability of the water sector:** Water processing instalments are vulnerable to unintentional and intentional physical and cyber threats. Cybersecurity threats in this sector are increasing. Effects of threats could lead to deaths of people by poisoning, spread of infectious diseases, economic damage, and loss of trust to providers and governments.
- **Cyberthreats are present and increasing:** The cyberattack on the Oldsmar water treatment system in the USA in 2021 demonstrated that some malicious actors intend to poison water before it is distributed to thousands of households.[6] This attack also demonstrated that it is possible that malicious actors will not want money, but could be motivated by geopolitical concerns.

Resilience and regulation of cybersecurity in the sector:

- **Fragmentation of the sector:** The water management sector is very fragmented and disaggregated. Regulation of cybersecurity that is coordinated across the region is therefore very difficult in this sector.
- **Insufficient awareness of cyberthreats:** More needs to be done to raise awareness by numerous small companies of cyberthreats in this sector and the potential implications. It is clear that this is the case for both policy makers and operators, as for example an additional water management subsector (wastewater) had only been added as category to NIS2 and not the first NIS Directive (Directive concerning measures for a high common level of security of network and information systems across the Union).[7]
- **Limited resources for cybersecurity:** Discussions showed that cybersecurity is not a clear priority for all water providers. This sector faces a dilemma on how to balance limited financial resources for cybersecurity and increasing security needs. As a result, the sector often utilizes outdated information systems.

6 See Florida Water Treatment Plant Hit With Cyber Attack: https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/.
7 See The NIS2 Directive: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

- **Cybersecurity skills gap in the sector:** The water sector is fairly particular and there are not many experts dedicated to cybersecurity of water management systems. It is important to broaden the pool.

- **Limited information sharing:** Given scarce resources and limited cooperation, information sharing must improve. To that end, relevant experts need to cooperate long before an incident takes place, potentially through cybersecurity exercises to ensure trust is built over time. Trust cannot be mandated but earned. The discussion also highlighted that cybersecurity needs to be seen as a team activity and that the public and private sector need to find avenues to leverage its respective strengths and seek to collaborate in addressing common threats and challenges in cyberspace (the EU Joint Cyber Unit may evolve into such a platform).

- **International regulation is limited :** Approaches to cybersecurity regulation in this sector have been few and far between as governments view this sector predominantly as a local or national matter, though river management is a notable exception.

- **Cyber and physical security are interconnected:** Experts frequently focus on either physical security or cybersecurity at the expense of the other. The EU regulatory approach follows a similar model with the NIS2 Directive concerning measures for a high common level of cyber security of network and information systems and the CER Directive on the physical resilience of critical entities.[8] However, these two fields are interconnected and more focus should be given to bridging that gap.

- **Uneven implementation of cybersecurity measures across the EU:** Participants observed that the EU Member States have varied levels of cyberresilience and that they have implemented measures agreed upon at the EU level to differing extents. The EU should encourage all Member States to strive towards a higher level of cybersecurity across critical infrastructures.

The role of international law and norms:

- **Water management systems as targets:** Water management systems have been targeted in armed conflicts and wars. Parties in conflicts destroyed these systems to harm and forcefully move civilian population or to prevent the opposite side to use these objects as elements of warfare. This has typically been done kinetically and not in the online environment. However, as more and more water facilities rely on technology for efficient management and distribution, it is clear cyberattacks are a real possibility.

- **Water management systems as protected infrastructural entities:** Water management infrastructure is a civilian infrastructure and attacks on this infrastructure are prohibited by law, such as by the Geneva Conventions during armed conflict and through international cybersecurity norms in peacetime.[9]

- **Access to water:** Human rights law also applies to the water sector, as access to water is considered a basic human right. Interference with that access, through cyber or other means, could therefore be considered a breach of those rights and state obligations to protect them.

- **Breach of sovereignty:** In addition to other international legal concepts and frameworks, a targeted attack on the water management system could also be considered as a breach of sovereignty.

8 See Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities on the resilience of critical entities: https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

9 See The Geneva conventions: https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf.

WORKSHOP 02

Electric power infrastructure and services

Summary of key take-aways for policymakers and practitioners

Cyberthreats and risks to the sector:

- **Criticality of the electric power:** Electric power is a basic human resource. This means that most human activities directly or indirectly depend on it. Consumers range from billions of households to high voltage consumers, such as factories.

- **The electric power sector is central to most critical infrastructure:** Should the result of a cyberattack on the electric power sector be a blackout, many sectors, including much critical infrastructure, will be affected. We should expect cascading effects in particular if a blackout lasts for an extended period of time. The ultimate worst-case scenario is the so-called Black Sky scenario, where a blackout could last for a month or longer. This possibility is underestimated by most decision makers and social consequences insufficiently explored.

- **Electric power systems are vulnerable to cyberattacks:** Electric power systems generate power in many ways and store electricity and transmit it to users through power grids. All phases of this process are enabled by technology and can consequently be attacked. Just two days before the webinar, the then most devastating cyberattack on U.S. infrastructure to date took place. In this particular case, a ransomware attack temporarily shut down the Colonial Pipeline.[10] The pipeline supplies around 45 % of fuel consumed daily on the U.S. East Coast. The pipeline's service was soon restored, but this attack should be taken as a warning sign that future ones could be even more disruptive. The ongoing situation in Ukraine provides another stark illustration of how electric power plants and other systems can be targeted and damaged. Over the past years, attacks on Ukrainian electricity services have severely damaged infrastructure and created serious societal consequences.

Resilience and regulation of cybersecurity in the sector:

- **High interdependence between information and communication technology and electric power:** Electric power has a unique relationship with information and communication technology because of the strong interdependence between the two sectors. Electricity is essential for ICT to operate, and ICT is now vital to the electric power grid. This interdependence should be further examined.

10 See Hackers Breached Colonial Pipeline Using Compromised Password: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

- **Past attacks as stimulus for cyberresilience:** Experience shows that organizations often only act in response to a successful attack. Moreover, attacks on critical infrastructure often help uncover deficiencies in national legal or regulatory frameworks. It is also important to look beyond a particular attack, as the next one might be different. Some observers identified a lack of imagination by some governments when it comes to understanding what future cyberattacks could look like.

- **Limited awareness of cyberthreats:** In some cases, observers reported a lack of awareness of the prevalence of cyberthreats and the importance of investments in cybersecurity in the electric power sector.

- **The role of voluntary measures:** Compliance should not be the main motivation driving cybersecurity investments. The role of voluntary solutions in raising the levels of cyberresilience is underestimated.

- **Cybersecurity as a path and not an end:** Cybersecurity requires constant investment and innovation to keep pace with advances in technology.

- **Cybersecurity is ultimately about people:** It is relatively easy to improve technical cybersecurity systems, however it is very difficult to build a culture of cybersecurity among personnel and users.

- **Information sharing as key to success:** We need more intra-sectoral, cross-sectoral and cross-border information sharing. The Dutch government's approach should be considered as a good practice, as they ensure that government shares information with the private sector and vice versa.

- **Cooperation is important at national as well as at the EU level:** It seems that cooperation in the electric power sector works rather well at the national level in a number of countries, but that still has to be translated to the EU level. It is important to acknowledge that building communities of trust takes time.

The role of international law and norms:

- **Organizations often play more than one role in cybersecurity:** Governments can be perpetrators of cyberattacks, regulators, and also defenders of their citizens against attacks. Companies on the other hand can be the vector, the victim, and field of war.

- **Rules governing state-driven or sponsored action in cyberspace:** A cybersecurity framework that outlines what state-led actions are allowed and what states are obliged to do in cyberspace has been agreed upon, but there are significant gaps that need to be still addressed. Moreover, states need to ensure that they implement agreements, as well as hold perpetrators accountable for breaches.

- **Rules need to be exercised:** International agreements can only be successful if they are used—this applies to international law and cybersecurity norms. Currently states are reluctant to enforce the frameworks and are still determining how they are interpreting key concepts. Understanding not only what states are doing, but what is guiding their decisions will be important.

- **General frameworks are hard to apply to specific context:** Without states utilizing the international legal frameworks, we do not know how to apply them to specific areas, such as the power grid. It also means that we are not certain all aspects are covered under these frameworks—they need to be tested.

- **A combination of norms and international law is needed:** The international framework is likely to still evolve as technology evolves. A combination of binding and voluntary rules is essential at this stage.

WORKSHOP 03

Health infrastructure and services

Summary of key take-aways for policymakers and practitioners

Cyberthreats and risks to the sector:

- **Criticality of public health:** Access to healthcare is a human right. Healthcare services, whether provided through hospitals, nursing homes, pharmacies, etc. are vital for our society. Increasingly, and in particular over the past two years as we focused on social distancing, the delivery of healthcare is supported or enabled by technology.

- **Rising cyberthreats:** The COVID-19 pandemic has dramatically increased the online threats to this sector. As healthcare institutions strained under the weight of the pandemic, the raising cyberthreats made the situation even more difficult to manage. For example, ransomware has been deployed against the healthcare sector. Medical records continued to be a lucrative target for cybercriminals. Furthermore, data related to COVID-19 has risen in importance and become a tool of geopolitics—such as the valuable intellectual property for vaccines. Finally, state sponsored disinformation campaigns with a focus on healthcare, undermined our response to COVID-19.

- **The impact of cyberattacks in this sector is palatable:** Attacks on hospitals are not attacks on nameless institutions. These attacks impact patients, potentially delaying their healing process or putting their lives at risk.

- **Attackers act with impunity:** As in other sectors, malicious actors that target hospitals online are rarely caught and punished. However, attacks here can be particularly damaging.

Resilience and regulation of cybersecurity in the sector:

- **Continuity of service needs to be a key focus for healthcare systems:** Patient care is the highest priority for healthcare systems, which is why ransomware attacks on hospitals are so concerning. If a hospital is not able to continue to provide care, lives can be at risk.

- **Cybersecurity has not been the highest priority:** Investment in cybersecurity in this sector has been too low. Finances are often stretched and areas for investment need to be prioritized. Given its mission, the focus is first—and rightly so—on new equipment, drugs, etc. Moreover, managers are often medical professionals and do not see cybersecurity as a priority. However, that has meant that hospitals have embraced technology, but stopped short of integrating modern day cybersecurity protections.

- **Cyberattacks can act as a stimulus for resilience:** Evidence shows that organizations are often shocked into action following a damaging cyberattack. Unfortunately, some organizations only focus on modernization of legacy systems and prioritizing of good practice cybersecurity after an attack occurs.

- **Cyberhygiene needs to become a priority:** It is important to acknowledge that the healthcare sector needs to do more to become cyberresilient. We need proper investment in technology, good regulations, increased cybersecurity awareness of all staff, as well as regular cybersecurity exercises. These measures together could prevent a large share of cyberattacks.

- **An emerging approach at the EU level:** Healthcare remains a core competency at the national level. Nevertheless, cybersecurity cannot be achieved within national borders. Recognizing this, two interconnected directives are focused on raising resilience across the continent—beyond just the healthcare sector. The NIS Directive focuses on measures for a high common level of cyber security of network and information systems and the CER Directive focuses on the physical resilience of critical entities. In addition to these efforts, more needs to be done to connect national crisis management networks and share information in a timely manner.

The role of international law and norms:

- **International law can be leveraged to address threats against the healthcare sector:** The discussant made it clear that international law applies to this space and that actions that are prohibited in the real world (attacks on hospitals), should also be clearly prohibited in the online world.

- **More practice needed:** While theoretical approaches are clear, it is important that these are leveraged in practice to create clarity. The Oxford Process is one such example.[11] These discussions have revealed that cyberattacks on healthcare could represent not only a breach of international law or human rights law, but also a breach of sovereignty, or an intervention in internal affairs of the affected state. Due diligence could also be leveraged, as it would imply that the state from where the attack was carried out has obligation to deal with the actor.

- **Attributing cyberattacks:** Attribution has technical, political and legal dimensions. When using technical attribution, we follow the technical evidence to determine the origin of the attack. Legal attribution allows us to understand whether we have sufficient proof to use criminal frameworks to bring the perpetrators to justice. Political attribution on the other hand is leveraged by states when assigning an attack to a particular state and juggles competing geopolitical implications. Our technical ability to attribute cyberattacks has improved, both in terms of accuracy and speed. Legal frameworks have also been strengthened. However, given the political dimension involved, attribution remains a sensitive act.

11 See The Oxford Process: https://www.elac.ox.ac.uk/the-oxford-process/.

WORKSHOP 04

Financial infrastructure and services

Summary of key take-aways for policymakers and practitioners

Cyberthreats and risks to the sector:

- **Criticality of the financial sector:** The modern financial sector enables transactions by leveraging technology. Any interruption to these services can result in direct financial consequences, as well as numerous indirect consequences, such as loss of reputation and trust, lawsuits, etc. Given the centrality of the financial sector to the global economy, the impact outside the narrow sphere of high finance is very real.

- **Increasing cyberthreats against the financial sector:** The financial sector has been one of the most targeted sectors in cyberspace for some time. During the COVID-19 crisis, as even more of the transactions moved online—such as through e-banking—and as more bank employees worked from home, the attack surface grew. Attackers followed, executing increasingly sophisticated cyberattacks.

Resilience and regulation of cybersecurity in the sector:

- **Underinvestment in cybersecurity:** In comparison to other critical infrastructure sectors examined throughout the workshop series, the financial services sector is significantly more mature in its implementation of cybersecurity mechanisms. Nevertheless, all too often institutions still see cybersecurity as an unnecessary cost, or a nuisance that damages efficiency. It is not treated as a core part of the business.

- **Improved cyberresilience:** Existing levels of cyberresilience could be raised by improving information sharing, focusing on the public-private partnerships, investing in patching, updating out of date systems, implementing a segmented network structure that can help localize consequences of attacks, and limiting administrative access, amongst other things.

- **Effective information sharing:** Effective information sharing should contain at least the following elements: focus on voluntary sharing, identifying opportunities for cross-sectoral sharing, building trust among the actors involved, and ensuring there is clarity on who reports to whom and what happens with the data. FS-ISAC was noted as a particularly good framework for information sharing.[12]

- **Actionable incident reporting:** Incident reporting can be a helpful tool, but we need to shift from just exchanging and collecting data on cybersecurity incidents to distribution of actionable intelligence.

12 See Safeguarding the Global Financial System by Reducing Cyber Risk: https://www.fsisac.com/.

- **Existing EU initiatives:** There are several cybersecurity policy and regulatory initiatives that have been, or are in the process of being, adopted, at the EU level. We need to avoid duplication among different processes, harmonize the rules, and create risk-based proportional and non-prescriptive approaches. One such example is the interplay between the EU regulation Digital Operational Resilience Act (DORA) and the NIS2 directive. The former aims to ensure a comprehensive framework for cyber resilience in the financial sector at all levels. DORA contains requirements for risk management, reporting of ICT-related incidents, resilience tests, a supervisory framework, rules for the exchange of information, etc. NIS2 is similar in scope. It is important that the frameworks are not contradictory but aligned and reinforcing of each other.[13]

- **Cybersecurity cooperation in Europe:** The European Union and its focus on cybersecurity has ensured that Europe is likely the most advanced region in the world when it comes to information sharing amongst state actors. The practices implemented here are followed with great interest elsewhere.

The role of international law and norms:

- **Going beyond the international cybersecurity framework:** In 2021, states at the United Nations agreed upon an international framework for cybersecurity, consisting of 11 international norms and international law. These are broadly applicable and not specific to the financial sector. Beyond the international framework there might be a need for specific norms or frameworks that apply to the financial sector only (e.g., a norm on the integrity of financial systems and data has been proposed).[14]

- **Application of international law:** While discussions persist around how international law applies to cyberspace, some things are clear; international law in its entirety, including international humanitarian and human rights law, applies to this domain.

- **International agreements vs. established practice:** There is more than one way to build international norms and customs. One is to build agreements in international or regional fora and then expect states that have agreed to them implement those practices. The second is to start building expectations through direct actions, for example by pointing out malicious behavior whenever it occurs. This could over time equally lead towards an emergence of a norm.

- **Inclusion of insurance companies:** While typically not thought of as pure financial services, insurance companies may be able to provide helpful perspectives when it comes to international law, norms, and cybersecurity. Their experiences are wedded in risk management—online and offline. Moreover, with cybersecurity insurance becoming increasingly prevalent, insurance companies have been one of the first actors having to incorporate considerations of attribution and state-based attacks. War exclusions have therefore risen to the prominence in several insurance claims in recent years.

- **Norms in the age of fragmentation:** We need to pursue the goals of stability and integrity of financial sector by creating resilience norms that complement robustness norms.

13 See DORA (Digital Operational Resilience Act): https://www.grantthornton.ie/insights/factsheets/dora-digital-operational-resilience-act/#:~:text=DORA%20%28Digital%20Operational%20Resilience%20Act%29%2022%20Mar%202021,development%20of%20digital%20finance%20while%20mitigating%20associated%20risks. For NIS2, see: The NIS2 Directive: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

14 See Carnegie Endowment for International Peace - Cyber Policy Initiative Program: https://carnegieendowment.org/programs/technology/cyber/.

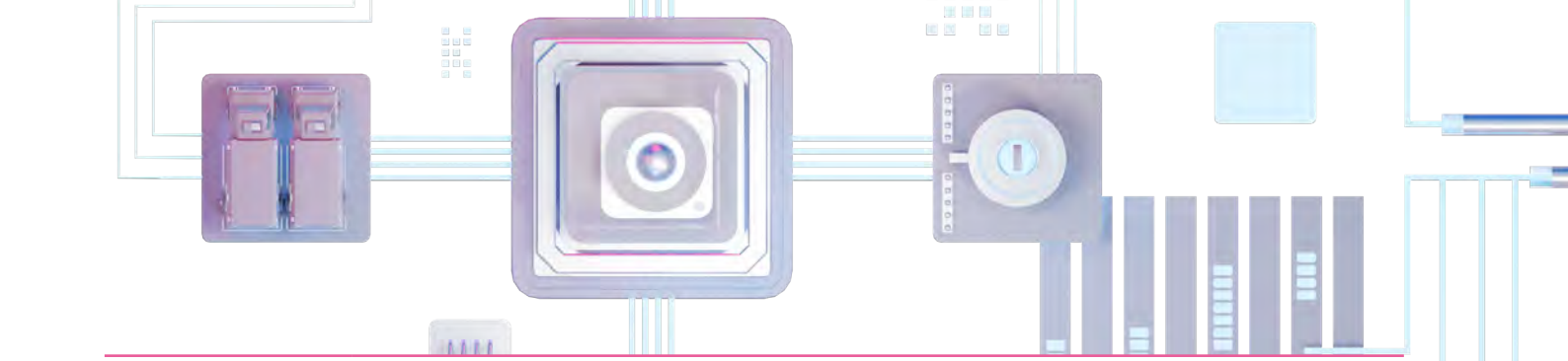
Speakers and Agendas of Workshops

The webinars were held under Chatham House rules and we therefore do not attribute any of the take-aways in this document to particular speakers or institutions.

WORKSHOP 01

Critical Infrastructure Protection: Cybersecurity and water

14:00 – 14:15	**Introductory remarks:** Uroš Svete, *Director of Information Security Administration, Slovenia*
14:15 – 14:45	**Online threats to the most precious of commodities: What can go wrong and what to do about it?** **Moderator:** Prof. Dr. Iztok Prezelj, *Faculty of Social Sciences, University of Ljubljana* Mark Montgomery, *Executive Director, Solarium Commission* Liga Rozentale, *Senior Director, Microsoft* Jože Tomec, *Head of Water Supply, Public Utility VOKA SNAGA*
14:45 – 15:30	**The role of regulation in improving water resilience: Slovenia, Europe and the world** **Moderator:** Ivana Boštjančič Pulko, *Directorate of Information Security Administration, Slovenia* Gorazd Božič, *Head of CERT Slovenia* Bart Groothuis, *Member of European Parliament* Dr. Evangelos Ouzounis, *Head of Unit – Secure Infrastructure and Services, ENISA* Isabelle Roccia, *Senior Manager, Policy, Business Software Alliance*
15:30 – 15:45	**Virtual coffee break**
15:45 – 16:30	**International law and norms: Are attacks on water off limits?** **Moderator:** Kaja Ciglič, *Senior Director, Microsoft* Nathalie Jaarsma, *Ambassador at large for security and cyber, the Netherlands* Sonja Koeppel, *Secretary of the Water Convention, UNECE* Dr Kubo Mačák, *legal adviser at the International Committee of the Red Cross (ICRC)* Tsvetelina van Benthem, *Oxford University*
16:30 – 16:45	**Conclusions:** Staša Novak, *Slovenian attaché for cybersecurity, EU & NATO*



WORKSHOP 02

Critical Infrastructure Protection: Cybersecurity and Energy

14:00 – 14:15	**Introductory Keynote:** Uroš Svete, *Director of Information Security Administration, Slovenia*
14:15 – 15:00	**Cyber threats to energy providers – what is hype and what is real? What's the best way to address the most imminent concerns?** **Moderator:** Prof. Dr. Iztok Prezelj, *Faculty of Social Sciences, University of Ljubljana* Dr Sanjay Bahl, *CERT India* Andrej Rant, *Head of Information Security, Eles* Trevor H. Rudolph, *Vice President for Global Digital Public Policy, Schneider Electric* Ievgen Vladimirov, *Deputy Minister Energy of Ukraine*
15:00 – 15:45	**Resilience and regulation – what are the opportunities and challenges for an EU framework for energy cybersecurity guidelines?** **Moderator:** Florian Pennings, *Director, Microsoft* Mireille Kok, *Head of Unit Cooperation, NCSC, The Netherlands* Evangelos Ouzounis, *Head of Policy Development and Implementation Unit, ENISA* Massimo Rocca, *Chair of EE ISAC*
15:45 – 16:00	**Virtual coffee break**
16:00 – 16:45	**International law and norms: What is off limits and what is lawful?** **Moderator:** Marko Rakovec, *Director General for International Law and Protection of Interests, Ministry of Foreign Affairs, Slovenia* Kaja Ciglič, *Senior Director, Microsoft* Duncan Hollis, *Temple University* Andraž Kastelic, *UNIDIR*
16:45 – 17:00	**Concluding Keynote:** Lt Gen Rajesh Pant, *Head of National Cyber Coordination Centre, India*

WORKSHOP 03

Critical Infrastructure Protection: Cybersecurity and Healthcare

13:00 – 13:10	**Introductory Remarks:** Uroš Svete, *Director of Information Security Administration, Slovenia*
13:10 – 13:55	**From hospitals, to vaccine manufacturers, to ministries and international institutions – cyberthreats are real. What can we do about it?** **Moderator:** Liga Rozentale, *Senior Director, European Governmental Affairs, Microsoft* Stéphane Duguin, *Chief Executive Officer, CyberPeace Institute* Petr Novotny, *Director of the Cyber Security Policy Department, NÚKIB, Czech Republic* Flavio Aggio, *Chief Information Security Officer (CISO), World Health Organization (WHO)*
13:55 – 14:40	**Resilience and regulation: What are the opportunities and challenges for an EU framework for healthcare cybersecurity guidelines?** **Moderator:** Thomas Boué, *Director General, Policy – EMEA, Business Software Alliance* Eva Telecka, *Director, IT Security & Risk Management EMEA, MSD* Staša Novak, *Cyber Attaché to EU and NATO, Permanent Representation of the Republic of Slovenia in Brussels* Kuba Boratynski, *Head of Unit, Cybersecurity and Digital Privacy Policy, Directorate-General for Communications Networks, Content and Technology, European Commission*
14:40 – 15:20	**Attacks on healthcare are banned under the laws of war. Is it time to ensure the same is true for peace time?** **Moderator:** Prof. Dr. Iztok Prezelj, *Faculty of Social Sciences, University of Ljubljana* Anne-Marie Buzatu, *Vice-President and Chief Operating Officer, ICT4 Peace* Kaja Ciglič, *Senior Director, Microsoft* Michael Schmitt, *Professor of International Law at University of Reading* Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial, *Professor of Law, Director, National Security Law Center, University of Virginia*
15:20 – 15:30	**Concluding Keynote:** Mr. Richard Kadlčák, *Czech Republic´s Special Envoy for Cyberspace*

WORKSHOP 04

Critical Infrastructure Protection: Cybersecurity and Finance

14:00 – 13:15	**Introductory Remarks:** Uroš Svete, *Director of Information Security Administration, Slovenia*
14:15 – 15:00	**Protecting the global financial systems online – finding the weakest link** **Moderator:** Ivana Boštjančič Pulko, *Information Security Administration, Slovenia* Matthew Field, *Executive Director, JP Morgan Chase* Tamas Gaidosh, *Financial Regulation and Supervision Division, IMF* Helena Pons-Charlet, *Senior Corporate Council, Digital Crimes Unit, Microsoft* Boris Vardjan, *CISO, NKMB and Leader of the Security forum for IT of Bank Association of Slovenia*
15:00 – 15:45	**Resilience and regulation: Global financial system meets regional approaches – what is the best path forward?** **Moderator:** Florian Pennings, *Director, European Governmental Affairs, Microsoft* Vangelis Ouzounis, *Head of Policy Development and Implementation Unit European Union Agency for Cyber Security, ENISA* Jason Harrell, *Head Of External Engagements, Operational and Technology Risk, Depository Trust & Clearing Corporation* Alexandra Maniati, *Director, Innovation & Cybersecurity, European Banking Federation* John Salomon, *Regional Director for continental Europe, Middle East, and Africa at the FS-ISAC*
15:45 - 16:00	**Virtual Coffee Break**
16:00 – 16:45	**State driven attacks against financial system can threaten the global economy: Do we need new norms to reign them in?** **Moderator:** Prof. Duncan Hollis, *Temple University* Kaja Ciglič, *Senior Director, Microsoft* Kathryn Jones, *Head of International Cyber Governance, UK FCDO* Ariel Levite, *non-resident fellow, Carnegie Endowment for International Progamme*
16:45 – 17:00	**Concluding Keynote:** Prof. Dr. Iztok Prezelj, *Faculty of Social Sciences, University of Ljubljana*