RESEARCH IN FOCUS

Global Cyber Resilience: thematic and sectoral approaches

Kate Saslow
Stiftung Neue Verantwortung
October 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Acknowledgments

Many thanks to Sven Herpig and Patryk Pawlak for the detailed exchange over this paper, as well as their support in research and logistics of project planning. Thank you as well to all the experts who participated in the workshops of the EU Cyber Direct project. Your knowledge is integral and invaluable.

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).

Abstract

This paper looks beyond notions of cybersecurity and analyses a more holistic approach to fostering resilience in cyberspace. This analysis has multiple goals: First and foremost, it seeks to achieve a common understanding of what resilience in cyberspace means and why it is important as a prerequisite to any collective action. Next, it looks at digital and cyber strategies within the European Union (EU) and at external action to better understand the current European approach to resilience. Then, it breaks down the state of play in order to isolate specific actions that promote resilience in an interconnected digital society. Only by understanding how the EU views resilience, and the capacity-building required to foster it, can methods to promote cyber resilience be discussed at a global level. Thus, both theme-based and sector-based approaches are addressed in this paper. Identifying best practices from companies, sectors, or regions is a way to identify exactly what works to build resilience. Then, with international cooperation and strategic partnerships, these methods can be scaled to make resilience and stability in cyberspace a global goal. This analysis sets up the discussion for key stakeholders to work toward a global cyber resilience regime.

Key points

- Promoting resilience in cyberspace should be a collaborative and global effort.
- Although different actors may have different understandings of what exactly resilience in cyberspace means, there are certain measures that can be promoted everywhere which lead to more resilient societies and digital ecosystems.
- As a key stakeholder, the European Union should foster both internal and external resilience initiatives – especially around measures such as risk management, adaptation, and information-sharing – to protect the stability of cyberspace.
- Investing in an international resilience framework is an effective and far-reaching strategy to strengthen the stability of cyberspace for everyone.

1. Introduction

The increased digitalisation in the previous decade has been fraught with data breaches, cyber espionage, meddling in democratic processes and compromising critical infrastructures - all phenomena still present in today's world. Organisations and countries are moving beyond the traditional notion of cybersecurity, with its firewalls and antivirus software, but much more is needed for a strategic framework for resilience in cyberspace. Revisiting some of the cyberattacks of 2017 and 2018, including WannaCry, NotPetya and Equifax, shows either that too much confidence has been placed in traditional ICT maintenance measures or that there has been a lack of awareness about how to prevent such highly damaging breaches. Implementing stronger defensive mechanisms that are designed to prevent and reduce damage - and recover quickly through flexibility - is essential. Therefore, when exploring new avenues to better protect an increasingly digitised world, the focus should be on comprehensive and ambitious resilience.

Organisations and countries are moving beyond the traditional notion of cybersecurity, with its firewalls and antivirus software, but much more is needed for a strategic framework for resilience in cyberspace.

Resilience as a buzzword is not novel. In nature, a reed is more resilient than a tree in a storm, as it bends and does not break and, thus, recovers rapidly. As a biological concept, resilience is commonly used to describe the capacity of an ecosystem to respond to and recover (even with increased strength) from a disturbance. Take a virus like influenza A and B, for example: This common virus can produce one to 10,000 copies of itself within 10 hours. Eventually, a virus with a mutation is created, and this mutation can render the virus resistant to whatever vaccine may be in its host's body. Within a short span of time, that mutation can spread and the virus will have successfully adapted to the immunity of its host. Resilience in this case then also means that the immune system (ecosystem) grows stronger after successfully recovering from the flu. This is not to say that no future infection or virus will disrupt the immune system, but rather that the system has a higher threshold for disruption and resilience, making the future of the immune system more capable of coping with and recovering from any disruption or threat. Drawing analogies between the biological representation of resilience and its potential role in better protecting our increasingly digitised and ICT-reliant societies is not far-fetched, as Ito and Howe discussed in *Whiplash: How to Survive Our Faster Future*[1].

Resilience becomes a matter of international solidarity and common approaches.

Many countries are currently looking into fostering resilience, but generally these efforts need to be increased. Moreover, as cyber disruptions increasingly cross borders and spread rapidly across the globe, resilience becomes a matter of international solidarity and common approaches. Indeed, it becomes more important for protection of a global digital economy and society. As a stakeholder, the European Union needs to take an even more strategic approach to building a resilience framework in cyberspace. This means increasing education efforts, information-sharing, rapid response, recovery and backup facilities, long-term planning, joint trainings and exercises and other mechanisms to increase resilience both in the EU and with strategic partners in the global Internet ecosystem. Strategic partnerships can enable affected stakeholders to more efficiently increase their resilience, thus creating a more robust ecosystem worldwide. Resilience at the international level is leveraged here in order to improve resilience at subsidiary levels. This means that analysing initiatives internationally with a

[1] Analogy from Joi Ito & Jeff Howe, Whiplash: How to Survive Our Faster Future (New York: Hachette Book Group, (2019).

comparative lens, rather than just looking at transnational approaches, can serve the ultimate purpose of increasing the digital resilience of the EU's economy, society and democracy.

This paper aims to aggregate the current discussion around resilience in the EU and serves as both a starting point and a problem analysis for discussing what the next steps would be for increasing resilience in cyberspace within the EU and in cooperation with strategic partner countries. Firstly, the paper identifies the current working definition of resilience. Having a common understanding of what resilience means - and what the concrete components of the definition actually mean - is the first step for developing more effective approaches to resilience. Secondly, it presents a strategic perspective on resilience serving as a broader framework for future actions by the EU. Furthermore, it identifies measures that could lead to increased resilience within the EU and for strategic partners. And lastly, the paper suggests two mechanisms which could be leveraged for EU international cooperation to further explore a plan of action for the EU to increase overall resilience of the Internet ecosystem.

2. What is Cyber Resilience and Why It Matters

First, it is crucial to have a common understanding of what exactly cyber resilience (often only referred to as "resilience") means. Resilience in cyberspace has been defined in an EU context as "the ability to continuously deliver the intended outcome despite adverse cyber events",[2] or as "the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack".[3] More broadly, resilience can be understood as "the ability to face shocks and persistent structural changes in a way that societal well-being is preserved".[4] Whereas cybersecurity is often considered as only protecting networks and IT systems against attacks (i.e. by implementing IT security tools or setting up security teams that deal with protecting a system) and preventing compromises, cyber resilience enables quick recovery after successful attacks (i.e. through secure regular backups) and, therefore, is an integral part of the IT system and organisational operation. Thus, resilience in cyberspace requires a more holistic approach in order to preserve societal well-being and ensure intended operations resume unphased.

> **“**
>
> **Organisations must also work towards cyber resilient strategies that enable their IT ecosystem to quickly recover in response to such attacks.**

When considering WannaCry as a resilience failure, the transnational nature of cyberattacks and the need for international cooperation becomes clear. The WannaCry ransomware attack in May 2017 was reported to have affected over 200,000 computers across 150 countries. WannaCry and the subsequent NotPetya attack spread like an epidemic and caused major operational disruption, even affecting health services and other critical infrastructures.[5] Although not every cyberattack is of the same nature, many attacks result in operational disruption. Therefore, on top of measures focused on preventing, detecting and reacting to attacks, organisations must also work towards cyber resilient strategies that enable their IT ecosystem to quickly recover (and grow stronger) in response to such attacks. Such strategies would facilitate IT

[2] Fredrik Björck et al. „Cyber Resilience – fundamentals for a definition“, Stockholm University, Department of Computer and Systems Sciences (2014). https://www.researchgate.net/profile/Janis_Stirna/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition/links/56824da408ae1e63f1eed116/Cyber-Resilience-Fundamentals-for-a-Definition.pdf.

[3] European Central Bank, “What is cyber resilience?”, Payment & Markets. https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html.

[4] EU Science Hub, “Resilience”, European Commission (2019).https://ec.europa.eu/jrc/en/research/crosscutting-activities/resilience.

[5] M. Wall & M. Ward, “WannaCry: What can you do to protect your business?”, BBC News, 19 May 2017. https://www.bbc.com/news/business-39947944.

security as well as national security. In addition, organisations - and, for that matter, states - might consider deterrence mechanisms like sanctions[6] or indictments, though these fall outside the scope of this paper. When WannaCry and NotPetya hit, fast recovery was not the case for many victims: Operations at the global logistics company Maersk and Britain's hospital infrastructure, for example, were affected for an extended period.[7] A lack of up-to-date systems was one security flaw. However, not having sufficient compartmentalisation, backups or fallback systems in place were among the main reasons for the resilience failure. Otherwise, the damage could have been mitigated.[8]

Table 1: Definitions of resilience from different contexts

Biology	Psychology	European Commission: EU Science Hub	European Central Bank
In **biology**, *resilience* is commonly used to describe the capacity of an ecosystem to respond to and recover (even with increased strength) from a disturbance.	In **psychology**, *resilience* refers to the process of adapting well in the face of adversity, trauma, tragedy, threats, or significant sources of stress.	The **European Commission's Joint Research Centre (JRC)** defines *resilience* as the ability to face shocks and persistent structural changes in such a way that societal well-being is preserved, without compromising the heritage of future generations.	The **European Central Bank** defines *cyber resilience* as the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack.

In its 2016 resilience factsheet, the European Commission describes resilience as the "ability of an individual, a household, a community, a country or region to withstand, cope, adapt, and quickly recover from stresses and shocks, such as violence, conflict, drought, and other natural disasters without compromising long-term development".[9] The Commission has also defined resilience in its *Joint Framework on countering hybrid threats* as the "capacity to withstand stress and recover strengthened

[6] The EU Cyber Diplomacy Toolbox for example, allows the EU to implement sanctions even without the collective EU attribution of an attack to a specific country. Restrictive measures such as sanctions, however, require member states to clarify the scope of the sanctioning regime before operationalisation of the toolbox. Another example of deterrence measures can be seen in the United States 2018 DoD Cyber Strategy and "defense forward", or "confronting threats before they reach U.S. networks."

[7] Chris Graham, "NHS cyber attack: Everything you need to know about 'biggest ransomware offensive' in history", The Telegraph, 20 May 2017.https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

[8] Scott Bekker, "Inside a Domain Controller Nightmare", Bekker's Blog, *Redmond Magazine,* 27 August 2018. https://redmondmag.com/blogs/scott-bekker/2018/08/domain-controller-nightmare.aspx.

[9] European Commission, "Building Resilience: the EU's approach - Factsheet", Brussels (2019). http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/resilience_en.pdf

from challenges".[10] The EU has also recognised increasing threats and risks in the cyber domain. There are many different components to a cyber resilient ecosystem, which is able to continuously deliver intended outcomes despite adverse events. Some specific fundamental characteristics of resilience in cyberspace can include risk assessment, adaptation and long-term thinking, effective communication and coordination, societal cyber hygiene, protecting and securing critical public infrastructure and incident exercises to prepare for specific fallouts and recovery. It is worth examining these components more closely to understand how they can be a part of the EU's framework for cyber resilience. Global efforts for resilience must consider how other key actors define and pursue resilience in the digital sphere.

The European definition of cyber resilience has key similarities and differences compared to how its strategic partners conceptualise it. One accepted definition from the United States, for example, refers to resilience in cyberspace as, "The ability to *adapt* to changing conditions and *prepare* for, *withstand*, and rapidly *recover* from disruption".[11] One unique feature of resilience according to the American understanding is the tight link to national security and the need to enhance resiliency for homeland security, on top of economic and societal benefits.[12] In Japan, cyber resilience is tightly linked to Internet of Things (IoT) security. Japan invests heavily in IoT technologies and wants to be able to deliver products and services safely, securely and reliably over time - even in the face of cyberattacks.[13] Similar to the US, Chinese cyber resilience also nods to national security. China's efforts for resilience and its "network security priorities are motivated, just as all of China's myriad military modernisation priorities are, by the Chinese Communist Party's (CCP) primary goal of maintaining its own governing power. Ensuring domestic stability, territorial integrity, modernisation, and economic growth, while simultaneously preparing for the possibility of militarised cyberconflict in the future, are all objectives that directly or indirectly support the continuation of CCP rule".[14] Dissimilar to European, American and Japanese resilience efforts however, China prioritises sovereignty above international cooperation. However, for a global resilient digital economy and society, efforts among like-minded states should be leveraged where similarities exist - as well as fostering discussions about where differences lie - in order to promote resilience as broadly as possible.

Currently on the international level, leading roles in promoting measures to build resilient cyber ecosystems lie within certain multi-stakeholder institutions, namely the Global Commission for Stability of Cyberspace (GCSC), the Paris Call for Trust and Security in Cyberspace, the Siemens Charter of Trust, and the Global Forum on Cyber Expertise (GFCE). In their Singapore Norm Package from the 2018 summit, the GCSC discussed international norms for enhancing the resilience and integrity of cyber infrastructure.[15] The Paris Call, while not explicitly discussing cyber resilience, underlines the need to enhance digital cooperation and increase capacity-building measures and encourage initiatives that

[10] European Commission, "Joint Framework on countering hybrid threats: a European Union Response", Brussels, 6 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

[11] Office of the Director of National Intelligence, "Cyber Resilience and Response", Public-Private Analytic Exchange Program (2018). https://www.dni.gov/files/PE/Documents/2018_Cyber-Resilience.pdf.

[12] Ibid.

[13] William Saito, "Turning challenges of cybersecurity into new opportunities for growth", Japan Times, 20 January 2016. https://www.japantimes.co.jp/news/2016/01/20/business/turning-challenges-cybersecurity-new-opportunities-growth/#.XV-0CHtCSUl.

[14] Amy Chang, "Warning State: China's Cybersecurity Strategy", Center for a New American Security (2014). https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142.

[15] Global Commission on the Stability of Cyberspace, "Norm Package Singapore" (2018). https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjKvpfg2MzgAhXRDOwKHc0GCwcQFjAAegQICRAC&url=https%3A%2F%2Fcyberstability.org%2Fwp-content%2Fuploads%2F2018%2F11%2FGCSC-Singapore-Norm-Package 3MB.pdf&usg=AOvVaw3wCe1nqydwIMrdmvnCLpDl.

build *user resilience* and capabilities.[16] The Charter of Trust, launched by Siemens in 2018 to promote industrial security, has recently extended beyond an alliance of governments and universities to now include suppliers as well. Charter of Trust members have agreed upon baseline requirements to make cybersecurity a crucial aspect throughout all stages of the digital supply chain. According to the Charter of Trust, these requirements address all aspects of cybersecurity, including people, technologies and processes.[17] The GFCE is a global platform for countries, international organisations and private companies to exchange and develop best practices and to then scale them at the global level. One recent initiative in particular, the Internet Infrastructure Initiative, is to build a robust, transparent and resilient Internet infrastructure as a way to lead to more confidence and trust, increase the use of the Internet and even boost innovative and economic activities.[18] An overview of these holistic approaches on the international and multi-stakeholder level is one step towards moving to truly cyber resilient practices and eventually promoting them as global norms.

Having a definition of resilience is not only important to understanding what it means in a digital ecosystem, but also how to implement practices to promote it, as well as how to improve it. Looking at the European Union as an Internet ecosystem is one way to understand initiatives that are currently promoting resilience, as well as mechanisms to improve the resilience of cyberspace.

Table 2: International multi-stakeholder initiatives that enhance resilience

Global Commission on the Stability of Cyberspace (GCSC)	Paris Call for Trust and Stability in Cyberspace	Siemens	Global Forum on Cyber Expertise (GFCE)
Singapore Norm Package: discusses six international norms, some of which seek to enhance resilience in cyberspace, such as the Norm to Create a Vulnerability Equities Process, Norm to Reduce and Mitigate Significant Vulnerabilities, and Norm on Basic Cyber Hygiene as Foundational Defense. (2018).	**Paris Call:** reaffirms support of an open, secure, stable, accessible and peaceful cyberspace, which it recognizes is an integral component of life in all its social, economic, cultural and political aspects. (2018).	**Charter of Trust on Cybersecurity:** advocates ten principles with three objectives: protecting the data of individuals and companies; averting harm from people, companies and infrastructures; and establishing a reliable basis where confidence in a networked, digital world can take root and grow. (2018).	**Internet Infrastructure Initiative:** launches initiatives to bring stakeholders together, raise awareness and provide support for developing standards that foster a secure and resilient internet infrastructure. (2017).

[16] Globsec, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", 12 November 2018. https://www.globsec.org/cybersecurity-call-for-trust-and-security-in-cyberspace/.

[17] Nick Flaherty, "Siemens expands its cybersecurity charter activities to suppliers", EE News Europe, 15 February 2019. https://www.eenewseurope.com/news/siemens-expands-its-cybersecurity-charter-activities-suppliers.

[18] Global Forum on Cyber Expertise, "Internet Infrastructure Initiative". https://www.eenewseurope.com/news/siemens-expands-its-cybersecurity-charter-activities-suppliers.

3. Cyber Resilience in the European Union

> **Establishing a cyber resilient system requires both internal and external action for the EU.**

As early as 2013, the EU recognised the need for achieving resilience, defining it as one of five strategic priorities for an open, safe and secure cyberspace.[19] The Cybersecurity Strategy of the European Union stated that "to promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively".[20] Establishing a cyber resilient system requires both internal and external action for the EU. Public authorities and the private sector must cooperate effectively and develop capabilities to help counter cyber risks and threats, which have an increasingly cross-border nature.

The Organization for Security and Co-operation in Europe (OSCE) released a Decision in 2016 on "Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies".[21] This Decision adopted a number of CBMs (confidence-building measures) to build on work already being done by the OSCE, such as sharing information and facilitating inter-state exchanges in the form of workshops, seminars, roundtables and more. These are meant to enhance cooperation, transparency, predictability and stability - all of which are paramount for increasing resilience. These CBMs around ICT devices and their potential risks can also be transferred to a European Framework on promoting resilience.

The "Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises"[22] ("Blueprint") from 2017 is part of a European Commission Recommendation that adds to the initiatives on cyber resilience in the EU. The Blueprint presents guiding principles for responding to cyber incidents by presenting core objectives of cooperation at different levels as well as the actors and mechanisms involved. The core objectives of cooperation (effective response, shared situational awareness and public communication) at different levels (strategic/political, operational and technical) are principles that can not only be promoted inward as a blueprint for resilience within the EU, but also transferred to activities on a global scale. Promoting cooperation, communication and initiatives at different levels of society are all activities that promote a resilient cyberspace.

Similarly, in 2017, the European Commission released the Joint Communication to the European Parliament and Council on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". Underlining the importance of resilient practices in cyberspace, the Communication states that about 95 percent of incidents are enabled by a form of human error (intentional or unintentional), which shows the strong human factor in cyber incidents.[23] It is logical, then, to conclude that cybersecurity is everyone's responsibility and it is critical that corporate, public administration and personal entities

[19] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace" (2013). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001&from=EN.

[20] Ibid.

[21] Organization for Security and Co-operation in Europe Permanent Council, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1202 (2016). https://www.osce.org/pc/227281?download=true.

[22] European Commission, "Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises", Brussels, 13 September 2017. https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF.

[23] European Commission, "Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", Brussels, 13 September 2017.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

understand cyber threats and behave accordingly. It is necessary to nurture cyber hygiene habits in society; giving individuals the tools and skills to detect and protect themselves against attacks and encouraging businesses and organisations to adopt risk-based cybersecurity programmes are successful ways to do so. Furthermore, the Communication calls for Member States to make cyber awareness a priority in awareness campaigns that target schools, universities, business communities and research bodies.

In November 2018, the Council of the European Union updated the EU Cyberdefence Policy Framework. Updates include both implicit and explicit regards to resilience. In fact, the very first sentence of the updated framework reads, "To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cybersecurity and defence capabilities".[24] The framework notes that with cyberspace as the fifth domain of operations, EU missions and operations are "increasingly dependent on uninterrupted access to a secure cyberspace, and the EU thus requires robust and resilient cyber operational capabilities".[25]

This uninterrupted access to a secure cyberspace and the need for resilient cyber measures can further be understood as an important step to promote international action and partnerships. Cyber operations and malicious cyber activities know no borders, so EU efforts on resilience in cyberspace should look outward.

4. Thematic Areas for EU-International Cyber Resilience Cooperation

Promoting a global cyber resilient framework requires targeted actions and collaboration across sectors and borders. The European Union Global Strategy (June 2016) calls for "weaving cyber issues across all policy areas", further developing platforms for political, operational, technical cyber cooperation and more.[26] Promoting resilience with partners wherever possible is, thus, a useful strategy. Cooperation around resilience in cyberspace at the international level would be beneficial for the EU in order to exchange information gleaned from experience. Furthermore, capacity-building inside the EU - i.e. learning from international partners - and outside of the EU makes the internal EU ecosystem more resilient as well. What is needed is a practical approach to increase resilience. There are three themes in particular around which international resilience cooperation can effectively be built: 1) risk assessment; 2) adaptation, education and continuous learning; and 3) communication, information-sharing and coordination.[27]

> “
>
> **Cooperation around resilience in cyberspace at the international level would be beneficial for the EU in order to exchange information gleaned from experience.**

[24] Press release on a cyber defence policy framework, European Council, “EU Cyber Defence Policy Framework”, 19 November 2018.https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/.

[25] See 7

[26] The Global Strategy on the EU Foreign and Security Policy is a global strategy from the European Union on both global governance and external action in the 21st Century. https://eeas.europa.eu/topics/eu-global-strategy_en.

[27] Identified in an interdisciplinary multistakeholder workshop, these three themes were chosen as effective and realistic measures to boost collaboration to foster cyber resilience globally.

Risk Assessment

Incorporating risk assessment into the daily functioning of organisations, products or ecosystems shows that resilience requires an understanding of a system's potential weaknesses and then active protection of those vulnerabilities. Forecasting crisis and risk management will help make a system more resilient to any cyber incidents. The National Cyber Security Centre in the UK emphasises the importance of risk management as it helps "create plans for the future in a deliberate, responsible, and ethical manner", and is about "analysing our options and their future consequences, and presenting that information in an understandable, usable form to improve decision making".[28] Risk assessment can be understood as one part of risk management. According to the National Institute of Standards and Technology (NIST) in the US, the purpose of risk assessment is to identify:

- "(i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;"
- "(ii) vulnerabilities internal and external to organizations;"
- "(iii) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities;"
- "and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring)".[29]

The NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1, 2018) includes a Five-Function Framework for effective risk management: Identify, Protect, Detect, Respond and Recover. These five functions are meant to help organisations easily express their management of cybersecurity risk and enable risk management decisions.[30] In addition to activities in the US and UK, in the EU, risk assessment and risk management are central concepts in legal obligation such as EU cybersecurity and data protection legislation, notably the Network and Information Security (NIS) Directive and the General Data Protection Regulation. The NIS Directive - the first EU-wide legislation on cybersecurity - has three central objectives, one of which is risk management. The Directive establishes obligations for both operators of essential services (sectors such as health, transportation, energy, etc.) and digital service providers. Obligations include risk assessment and incident reporting. With this legislation, the EU says that understanding, assessing and communication risks with national authorities and international partners is a necessary step along the way to network security and overall cybersecurity. The Directive mandates the appointment of one national competent authority, a national Computer Security Incident Response Team (CSIRT), as a point of contact for liaising with other member states in order to institutionalise risk assessment and management on the national and international level within the EU.[31]

In order to ensure proper risk assessment and management within a system (country, institution, company, etc.), conversations must transcend the technical realm. Practitioners working in cybersecurity or IT security most likely understand the need to know a system, and where vulnerabilities within that

[28] The National Cyber Security Centre UK. "The fundamentals of risk," Risk Management Guidance (2016). https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals.

[29] US Department of Commerce, "Guide for Conducting Risk Assessments" National Institute of Standards and Technology, NIST Special Publication 800-30, pp.5 (2012). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[30] US Department of Commerce, "The Five Functions", Cybersecurity Framework. National Institute of Standards and Technology (2018). https://www.nist.gov/cyberframework/online-learning/five-functions.

[31] European Commission, "Directive on Security of Network and Information Systems", Factsheet, Brussels, 6 July 2016. https://europa.eu/rapid/press-release_MEMO-16-2422_en.htm.

“

In order to ensure proper risk assessment and management within a system conversations must transcend the technical realm.

system may exist. Incorporating this same sort of strategic foresight within other spheres as well, particularly in professional and political environments, is a logical next step to improve risk assessment capabilities across a wider scope of citizens.

Cyber risk assessment within an enterprise provides a good example of how the discussion must transcend solely technical spheres and also be discussed among top leaders, as they are ultimately responsible for overseeing risk.[32] While they are often accountable for any business failure, many board members or top leaders may be far removed from daily challenges such as monitoring and assessing cyber risks. Deloitte consultants posit, "Those leaders who develop a deeper view into where their organisation stands when it comes to cyber risk can gain critical understanding for managing their business".[33] Moreover, sharpening risk assessment capacities among top business leaders "should result in becoming a more secure, vigilant, and resilient business".[34] Efforts to promote resilience among businesses should therefore include capacity-building among top leaders on cyber risk assessment.

Promoting cyber risk assessment in the political realm can be done through policy dialogues with governments, international organisations and other players in a multi-stakeholder manner. The Internet Governance Forum Best Practices from 2017 even suggested that nations "become serious about putting in place a robust risk management system, driven by a common cybersecurity strategy". Specifically, the IGF best practice on risk assessment calls for a country-wide vulnerability management strategy and policies to ensure "stakeholder transparency and accountability in ISP, DNS, and IXP communities".[35] The IGF holds that in the political realm, governments could step up efforts to inform businesses and entrepreneurs about cybersecurity risks and share best practices.

“

Having conversations, joint trainings and exercises and informing members of society in professional and political settings is one way to increase exposure, preparedness and resilience.

Another example of this debate at a political level would be discussing cybersecurity and resilience efforts at a forum such as the UN Security Council. Essentially, part of effective risk analysis, assessment and management comes from sparking the debate among as many people as possible. Cyber threats are not just a problem for technical professionals but span many sectors, regions, demographics, etc. Having conversations, joint trainings and exercises and informing members of society in professional and political settings is one way to increase exposure, preparedness and resilience.

In the EU, the coordination of cyber risk management in case of large-scale incidents and attacks includes collaboration from actors across all levels - from the technical to political - and is spelled out in the Blueprint for rapid emergency response.[36] The Blueprint acknowledges that cyber incidents can often be part of a broader crisis, both originating from and impacting other sectors. The Blueprint states that as cyber events transcend to the physical world, it is necessary to take appropriate measures - cyber and non-cyber mitigation activities - in order to respond to risks in a holistic way. This is why the Blueprint discusses mechanisms that function at the technical, operational and strategic/political levels.[37]

[32] Deloitte, “Assessing cyber risk: Critical questions for the board and the C-suite”. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-assessing-cyber-risk.pdf.
[33] Ibid.
[34] Ibid.
[35] Internet Governance Forum. “Best Practice Forum on Cyber Security 2017” (2017). http://www.intgovforum.org/multilingual/content/igf-2017-best-practice-forum-on-cybersecurity#_ftn4.
[36] European Commission, “Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises” (2017).
[37] Ibid.

Adaptation, Education and Continuous Learning

Adaptation and long-term thinking reflect the biological concept of resilience and a system's ability to adapt and grow stronger over time. Fostering resilience means considering a longer time horizon and not simply trying to protect against past or present cyberattacks or events. Unique to resilience in cyberspace (or a lack thereof in society) is that societal costs of non-resilient systems are externalised. Data breaches, cyberattacks and cyber insecurity as a whole no longer just affect one system. This will continue to be a problem and without mechanisms in place, it will continue to be self-inflicted. Education policy to promote adaptation and continuous learning on cyber issues is one way to promote resilience in cyberspace and counter the externalisation of societal costs. In fact, a failure to act could have a $120 trillion impact on the global GDP by 2030.[38] The need for an international framework on digital resilience is imperative.

Similar to promoting risk assessment, education initiatives are important to promote adaptability and long-term planning. Education, trainings and exercises and raising awareness are vital to creating a culture of resilience. Not only through changing behaviour, but also in making society more effective in how it engages with digital technologies.[39] Skill forecasting could be an example of long-term thinking; in a report on resilience oversight expectations, the European Central Bank explains the expectations for skills and accountability of senior management and board members by saying that annual resilience training should include incident response, current cyber threats such as (spear) phishing, social engineering and mobile security, as well as emerging issues.[40] Incentivising diversity in the workplace with exercises and procedural planning with so called "wild cards" or "injections" is another way to have a workforce that is adaptable and strategic in a digital world.

Education policy is necessary for promoting adequate skills, first and foremost because of the talent pipeline. Already in 2013 the UK's National Audit Office released a report saying that not only does the current pool of "[cyber] security-graduates"[41] and practitioners fall short, but also that it could be 20 years until this skill gap is addressed.[42] By incorporating cybersecurity into education policy or curricula, a culture of resilience could be fostered and the costs of a non-resilient cyberspace would no longer be externalised to society. Examples of a cyber resilient education policy can be seen with IBM, which requires all employees to complete digital trainings annually, which include secure treatment of client data, appropriate use of social media and recognising and avoiding threats, such as phishing attacks in emails.[43] Across the EU, the European Union Agency for Network and Information Security (ENISA) has established a Cyber Security Month as an awareness campaign to promote good cyber hygiene across

[38] Zurich Insurance Group, "Cost of ineffective and uncoordinated action on cyber-risks continues to rise", 12 September 2018. https://www.zurich.com/knowledge/topics/risk-management-in-focus/cost-of-ineffective-and-uncoordinated-action-on-cyber-risks-continues-to-rise?page_attributes_refMktURL=https%3a%2f%2fwww.zurich.com%2fknowledge%2farticles%2f2018%2f09%2fcost-of-ineffective-and-uncoordinated-action-on-cyber-risks-continues-to-rise.

[39] The Scottish Government, "Safe, Secure and Prosperous: A cyber resilience strategy for Scotland", 2015. https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/.

[40] European Central Bank, "Cyber resilience oversight expectations for financial market infrastructures", (2018). https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

[41] Marisa Viveros, "Cyber Security Depends on Education", *Harvard Business Review, 24* June 2013. https://hbr.org/2013/06/cyber-security-depends-on-educ.

[42] National Audit Office Report, "The UK cyber security strategy: Landscape review", 12 February 2013. https://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/.

[43] Marisa Viveros, "Cyber Security Depends on Education", *Harvard Business Review, 24* June 2013. https://hbr.org/2013/06/cyber-security-depends-on-educ.

Member States. As part of the awareness campaign, ENISA created and maintains an NIS quiz to help citizens test their knowledge and support life-long learning on cyber issues.[44]

On top of education policy within a company or the current labour force, companies should be incentivised to look for future talent and future skills. This could also help bridge the gap in the talent pool and fill an empty pipeline. This topic was also discussed in the Joint Committee on the National Security Strategy for cybersecurity in the UK. One solution tabled was that the government should "seek to build the foundation of the future skills base, by nurturing both aptitude for those jobs that require only moderately specialist skills as well as core technical skills for those roles that require deep technical expertise".[45] However, just as risk assessment as a practice should transcend the technical sphere, a society's education system should be handled as a technical subject. It should also be included in business studies, legal studies, etc. in order to foster a culture of resilience at all levels of society.[46]

Communication, Information-Sharing and Coordination

Communication, information-sharing and coordination around cyber incidents is another fundament of resilience in cyberspace. This means not only having protocols and procedures in place, as well as sharing information within internal systems, but also effectively communicating threats and incidents externally with the populace. Explaining a crisis in a comprehensive way is a necessary first step to understanding its implications, as well as responding and reacting to it holistically. In this vein, communication must be both internal and external. Internally, organisations should collect information and consider information-sharing initiatives with other stakeholders. If key players share information on threats, vulnerabilities, attacks, etc., then the entire ecosystem can adapt, creating a more resilient digital economy and society. One particular policy that comes to mind when discussing this - which is also connected to the risk assessment theme - is the debate on government assessment, management, sharing and responsible disclosure of vulnerabilities.[47] This would be even more beneficial if the information-sharing efforts were not only cross-sectoral, but also cross-border. The World Economic Forum reports that the landscape of threat intelligence has historically been fragmented, with a high dependency on private-sector stakeholders and limited public-sector involvement. Increasing the outcome-oriented information-sharing to all stakeholders, and not limiting it within a single organisation, sector or even state, is one mechanism to improve internal communication and coordination to foster resilience, especially if this data-sharing is scalable and does not compromise sources or privacy.[48]

Externally, resilience in cyberspace relies on an effective communication and a baseline awareness level within society. Rather than systems simply "pulling" information (gathering and analysing information, for example), there should also be a way to channel this information to society, or "push" efforts. For

[44] European Agency for Network and Information Security, "Cyber Security Education", educational quiz. https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education.

[45] Joint Committee on the National Security Strategy, "Cyber Security Skills and the UK's Critical National Infrastructure", Second Report of Session 2017-19 (2018). https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf.

[46] Ibid.

[47] Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Process Around the World", *Lawfare Blog,* 4 January 2019. https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world. And Teodora Delcheva and Stefan Soesanto, "Time to talk: Europe and the Vulnerability Equities Process", European Council on Foreign Relations, 21 March 2018. https://www.ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process.

[48] World Economic Forum, "Research, data, and intelligence sharing", from the *Cyber Resilience Playbook for Public-Private Collaboration.* http://reports.weforum.org/cyber-resilience/research-data-and-intelligence-sharing/.

Resilience in cyberspace concerns the entire ecosystem, so communicating potential problems, threats and solutions with a wider populace is another theme to promote while discussing resilience.

too long, cybersecurity has been the purview of experts and technicians, who are not always trained to communicate the issues on top of fixing them. Framing the message to channel it or communicate with society is equally as important to achieving resilience. Message framing and a strategy for communicating a complex societal problem so that the core arguments are comprehensible should also be a priority of an organisation, be it a company or government.[49] Promoting digital literacy and good cyber hygiene within a society is a way to mitigate threats. This can be done by having two channels of communication. The first channel could be crowd-sourcing, or using society as active players in information- and threat-sharing. The second channel could be transparency from regulators when there are threats, attacks or other cyber incidents, and communicating this to the populace along with explaining the implications. Resilience in cyberspace concerns the entire ecosystem, so communicating potential problems, threats and solutions with a wider populace is another theme to promote while discussing resilience.

But the resilience of the European Union as a body also depends on other players in the greater cyber ecosystem. Promoting resilience internationally and not just within Member States is crucial.

5. Methods to Promote Cyber Resilience Globally

As shown, resilience plays a crucial role in securing the Internet ecosystem. But how can the European Union foster resilience internationally and push for a global cyber resilience regime? The EU provides the strategic framework for improving resilience with strategic partners through international cooperation. As discussed, useful thematic areas would be risk assessment; adaptation, education and continuous learning; as well as communication, information-sharing and coordination. Realistically promoting a cyber resilience regime globally means understanding which themes are an effective use of resources. With limited resources, identifying the best way to achieve a high level of resilience through international cooperation is crucial, as not every theme can be prioritised and undertaken at the same time. The remaining question is: How can concrete actions (both around these specific thematic areas and in general) be implemented to leverage international cooperation and boost resilience? Two methods in particular stand out: the *theme-based* and the *sector-based* approach. The *theme-based* approach looks at promoting resilience in the specific thematic areas discussed and acknowledges specific fora or organisations that currently work towards those goals. The existing initiatives could either be scaled or used as examples for future initiatives to make cyberspace more resilient for the EU and its strategic partners. Rather than considering different themes in isolation, however, the *sector-based* approach looks at a sector in which cybersecurity is of upmost importance to illustrate how multiple themes can be implemented in parallel to ensure resilience. Using a case study also shows best practices that could be scaled.

A. Theme-Based Approach

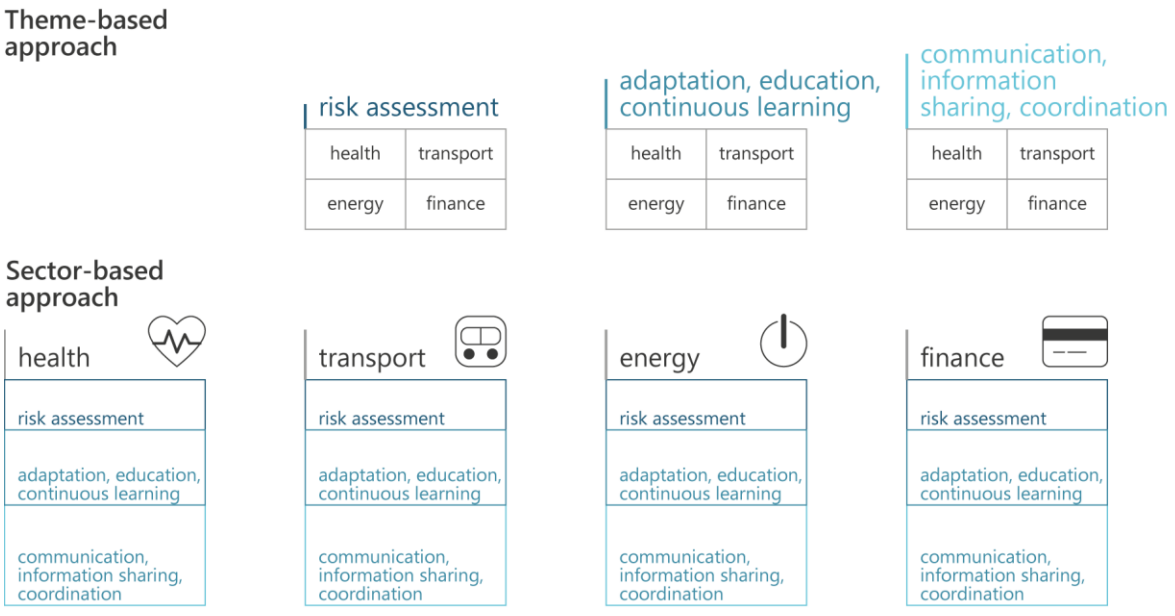
Using the three aforementioned thematic areas that help make a system more resilient as examples, the next step is to consider *how* to actually implement these activities. Understanding which international fora or cooperation frameworks currently exist is important here - the wheel must not be reinvented. Instead, existing fora can be leveraged to reach new goals.

[49] Hans de Bruijn and Marijn Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies", *Government Information Quarterly*, Vol 34(1) pp. 1-7 (2017). https://www.sciencedirect.com/science/article/pii/S0740624X17300540#bbb0020.

In promoting risk assessment, or making the technical debate more political and professional, certain political fora are good first resorts. Using international institutions like the G-7, the Global Forum on Cyber Expertise or other multitrack dialogues are good places to have the resilience debate at the international level. Current efforts include the "G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector", which serves as a set of "Fundamental Elements" for entities to adopt based on their specific risk profiles, operational and threat landscapes, roles in a given sector and legal or regulatory framework.[50] At the professional level, increasing risk assessment can be done in industry platforms by using trusted data pools and protected data-sharing, for example.

In fostering adaptation and learning, or upskilling, there currently are existing open-education resources that companies could pursue for their employees. Incentivising scholarships for such education initiatives, or providing financial resources to companies, would be ways to invest in an adaptable workforce, one that is equipped for the new and changing challenges presented by cyberspace. In fostering better communication, or information-sharing, leveraging the operations and coordination among different Computer Emergency Response Teams (CERTs) as part of the CSIRT network, after the implementation of the NIS Directive, could not only lead to a continuation of the successful EU-wide formal and informal information-sharing - it could also incentivise more international cooperation and further expand these best practices to strategic EU partners. This would lead to continuous effective responses to crises, increased transparency and comprehensive outreach to the public. An example of an existing information-sharing regime at the EU level can be seen within the energy sector. The Distributed Energy Security Knowledge (DEnSeK) is a European project for the creation of a Situation Awareness Network to share information on cyberattacks for a more resilient and secure EU energy sector.[51] Partnerships with strategic countries or bilateral relations can be used to develop information-sharing regimes and confidence-building measures between states. An existing international institution that could also be useful to promote communication among sectors and states is the Internet Governance Forum (IGF).

Figure 1: Theme-based or sector-based approaches



[50] See the non-binding principles of the "G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector". https://www.sciencedirect.com/science/article/pii/S0740624X17300540#bbb0020.

[51] European Union Agency for Network and Information Security (ENISA), "Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches" (2015).

In the 2018 IGF, one of the cybersecurity Best Practices called for the successful implementation of a collaborative model with trusted information-sharing "among and between stakeholders". Participation within this collaborative model should "extend not only to public and private sector entities who tend to own and control critical information infrastructure, but also stakeholders from other sectors (e.g. the banking and finance sectors, business process outsourcing (BPO), health, tourism, and energy sectors) and non-profit stakeholder groups (e.g. the technical community, academia, and civil society)".[52] Closer communication between the IGF, civil society and tech communities could also foster more resilience in cyberspace by bridging the gap between policy makers, society and practitioners.

“

Partnerships with strategic countries or bilateral relations can be used to develop information-sharing regimes and confidence-building measures between states.

B. Sector-Based Approach

An alternative to focusing on thematic areas that can be used to foster resilience across all sectors is to look more closely into specific sectors and illustrate the threats they face, as well as which mechanisms would be appropriate for fostering resilience in that specific sector. Take the health care sector, for example: In a report for the Wall Street Journal, Deloitte Insights reported that as of July 2016, health care attacks constituted 34 percent of all reported cyber breaches - higher than in any other industry.[53] Now, a year since the WannaCry attacks left the UK's health sector vulnerable, is a good opportunity to scrutinise the current state of affairs and think about how to strengthen the resilience framework to make sure that a sector as critical as this one can withstand any future adverse cyber events and carry on business-as-usual operations.

Countries' health sectors face myriad cyber threats and challenges. Communicating sensitive data among practitioners, dependence on uninterrupted access to critical infrastructure like water and electricity and the ubiquity of services and consumers are just a few examples of how far the health sector spans. A report from the Department of Health and Social Care from the UK government estimates that financial losses from the WannaCry attack amounted to a total of £92 million (in both lost output and IT costs in the 7-day period during the attack, as well as in the following months).[54] While looking specifically at the health sector, the thematic approaches to improve resilience mentioned above have more clear applications. Risk assessment could be facilitated among hospital staff, employees of an online platform that provides health services or even everyday users who rely on knowledge and services for proper care. Proactive threat detection abilities in the health sector are crucial, as they allow early discovery of breaches to help contain damage. Organisations can learn to leverage the knowledge of their business and functional environment in order to use analytical methods to detect patterns of behaviour and notice any deviations, allowing them to predict potential risks

“

Scenario exercises like "wild cards" could improve familiarity with crisis response and help identify areas for improvement in the case of an actual adverse cyber event.

[52] Internet Governance Forum, “IGF 2018 Messages - Cybersecurity, Trust and Privacy” (2018). https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1408

[53] Deloitte, “Cyber Resilience: Health Care's Best Defense”, The Wall Street Journal, 29 November 2016. https://deloitte.wsj.com/riskandcompliance/2016/11/29/cyber-resilience-health-cares-best-defense/?mod=rsswn.

[54] Department of Health & Social Care, UK Government. “Securing cyber resilience in health and care: Progress update October 2018” (2018). https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update.

sooner.[55] Adaptability and long-term thinking could also be applied to increase resilience in the health sector via skill forecasting and training exercises among hospital staff, for example, on what to do in the case of a cyber incident. Scenario exercises like "wild cards" could improve familiarity with crisis response and help identify areas for improvement in the case of an actual adverse cyber event.[56] Communication is also critical in the health sector. From doctors and hospital staff to users of online health apps seeking care, all rely on having information accessible to them. In the case of a cyber incident, this remains unchanged. Communicating clearly with those affected, as well as those responsible for responding to a cyber event is critical. Having incident response plans in place can help with this, especially when they clearly divide roles and responsibilities for all relevant internal and external stakeholders. This could include external legal counsel, third-party incident responders or public relations teams, among others.[57] Information-sharing with other institutions or organisations about where vulnerabilities lie or appropriate response processes is crucial to ensuring a resilient cyberspace in a vital sector of society. A similar approach for increasing cybersecurity on the international level is pursued by the Carnegie Endowment for International Peace with focus on the financial sector.[58]

The sector-based approach appears enticing as it is both holistic (within the sector) and scalable (adding additional sectors later by relying on an already tested approach). When taking an approach towards creating a global resilience regime, the EU needs to map existing initiatives in the arena to avoid duplicating efforts. This will also allow the EU to best utilise its strategic partnerships and leverage synergies.

6. Quo Vadis EU ?

Looking beyond the traditional notions of cybersecurity in today's increasingly digitised world is necessary. Whereas many players from different organisations, sectors or states may have conflicting views on what constitutes effective or sufficient cybersecurity, consensus on resilience is most likely easier to reach. At the international level, investing in cybersecurity may be difficult because the responses after an attack are restricted. For example, in the case of an international treaty on a secure cyberspace, if one state defects, the international community cannot do much more than impose sanctions.

With resilience, however, investing in an international framework means that even if a state defects from a treaty, the risks are not as high because states will have secured themselves through resilience measures. In the health sector, for example, a state can invest in cybersecurity measures and sign onto an international treaty barring states from attacking hospital infrastructures. But if a state defects, the consequences are severe. Whereas by investing in resilience in the health sector, the infrastructures, mechanisms and personnel are strong and resilient, so even if a state defects and attacks hospital infrastructure, the risks and consequences are significantly lower and the attack would likely not have lasting effects. This example also shows the value of international cooperation on resilience in cyberspace. Learning from the experience of another state, pooling resources and sharing best practices on both resilience mechanisms as well as information-sharing are specific international measures that could strengthen national resilience, even if one state were to defect from an international agreement.

[55] Deloitte, "Cyber Resilience: Health Care's Best Defense", The Wall Street Journal, 29 November 2016. https://deloitte.wsj.com/riskandcompliance/2016/11/29/cyber-resilience-health-cares-best-defense/?mod=rsswn.
[56] Ibid.
[57] Ibid.
[58] Michael Schmitt and Tim Maurer, "Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms", Carnegie Endowment for International Peace, 24 August 2017. https://carnegieendowment.org/2017/08/24/protecting-financial-data-in-cyberspace-precedent-for-further-progress-on-cyber-norms-pub-72907

Efforts on capacity-building and international cooperation around resilience are already in practice; learning from these initiatives is a way to benefit from best practices in building international trust when dealing with challenges. One example of collaboration around building resilience can be seen with the project, "Building Resilience to Tsunami in the Indian Ocean", funded from 2007 to 2009 by both the EU and sponsored by the UN International Strategy for Disaster Reduction. The project brought together NGOs, academic institutions and governments from Indonesia, Sri Lanka, India and the Maldives, four nations that were in the path of the South Asian Tsunami, which left them vulnerable and exposed to future disasters. Through objectives like making tsunami-threatened communities more aware of the risks and necessary actions; training local stakeholders in specific skills; establishing community-based infrastructure; preparing Information, Education and Communication (IEC) materials for awareness; and training and advocacy, stakeholders on the ground could develop a collaborative model and locally decide how to institutionalise risk-reduction processes.[59] While there have still been earthquakes in the region after the project ended in 2009, the societal impact of tsunamis has decreased as the population has become more resilient and capable of detecting, preparing for and responding to crises. This example is also a good reminder of the link between biological resilience and cyber resilience: Much like natural disasters, cyberattacks may be inevitable. Equipping society and key stakeholders with the tools and know-how to deal with such events and decrease their impact is, therefore, an effective way to enhance resilience in cyberspace. Identifying and mapping which initiatives already exist in order to foster a global cyber resilience regime is another step. This not only strengthens those initiatives already in place by sharing best practices, it also encourages other motivated actors to get involved.

> **“**
>
> **Learning from the experience of another state, pooling resources and sharing best practices on both resilience mechanisms as well as information-sharing are specific international measures that could strengthen national resilience.**

In the EU specifically, there are myriad benefits and interests in investing in a resilient regime, both internally and externally. International cooperation among key stakeholders is a sure way to build cross-sectoral and cross-border capacities on resilience. Strategic partnerships can boost collaboration so that actors can detect, prepare for and respond to crises and strengthen resilience in the international cyber regime.

About the author

Kate Saslow works at the intersection of technology and international policy. She currently works at the Stiftung Neue Verantwortung, a thinktank in Berlin, where she conducts research on resilience in increasingly digital societies in order to understand how international cooperation and cyber diplomacy can play a role. Additionally, she researches artificial intelligence and foreign policy as well as the information security of machine learning systems. She received her Master of International Affairs degree from the Hertie School in Berlin, where she specialised in topics of digitalisation, economic development, and governance, and concluded her studies with a capstone thesis on artificial intelligence and gender inequality in the United States labour economy.

[59] United Nations, “Building Resilience to Tsunami In the Indian Ocean: Action, Research, IEC and Practices”, International Strategy for Disaster Reduction (2009). https://www.unisdr.org/files/10910_BuildingResilience.pdf

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.