EU CYBER DIRECT

PROTECTING TRANSNATIONAL CRITICAL INFORMATION INFRASTRUCTURE: VITALITY, VULNERABILITY AND DIPLOMACY

Lise H. Andersen and Dennis Broeders

EU CYBER DIRECT

PROTECTING TRANSNATIONAL CRITICAL INFORMATION INFRASTRUCTURE: VITALITY, VULNERABILITY AND DIPLOMACY

Lise H. Andersen and Dennis Broeders

December 2023

Suggested citation: Andersen, Lise H., & Dennis Broeders (2023) *Protecting Transnational Information Infrastructure: Vitality, Vulnerability and Diplomacy*. Policy brief, EU Cyber Direct, December 2023.

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Cover image credits: Lars Kienle/Unsplash

Implementing organisations:

EU Institute for Security Studies
Carnegie Endowment for International Peace
Leiden University

Funded by the European Union

Contents

Executive summary

This paper, like the seminar on which it is based, considers how the governance of transnational critical information infrastructure (CII) could be approached at the global level. It suggests that when one is thinking about the (potential) governance of CII, it is important to recognise that not all infrastructure that is critical is also necessarily vulnerable. Thus, tailored approaches to its governance are required – as is shown to be the case with Internet Exchange Points. In addition, the paper concludes that there is no one-size-fits-all approach for the governance of different types of CII. The example of subsea cables makes it clear that for some CII, a deeper technical–political calculation accounting for the geopolitical context needs to be undertaken. Finally, the paper suggests that the EU could table a proposal at the Open Ended Working Group for a model of meetings that can be hosted under the Programme of Action. These meetings can bring together specialist technical knowledge and diplomatic expertise to advance understandings on topics that surface in the negotiations, including on issues of transnational CII governance.

Introduction: Protecting transnational critical information infrastructure

In its 2021 report, the sixth United Nations Group of Governmental Experts (GGE) elaborated the 11 norms of responsible state behaviour in cyberspace, which had previously been agreed in 2015. The enhanced understanding in this report of what the term *critical infrastructure* encompasses is the point of departure for this paper. Specifically, the GGE expanded its existing definition to include 'infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet'.[1]

There are two vital aspects to this broadened definition. Firstly, it acknowledges implicitly that critical information infrastructure (CII) is – at least partially – transnational in nature: if not the technical infrastructure itself, then at least in the fact that it provides services over multiple states. Secondly, it recognises, albeit indirectly, the importance of protecting the 'public core of the Internet' at the international level, and prompts consideration of a particularly challenging question:[2] given that some of the infrastructure underpinning the internet serves international populations, yet is located within the sovereign territory of individual states and is owned and operated by a multitude of actors, how should its governance at the global level be approached?

The importance of protecting the internet's infrastructure, and ensuring its functionality and integrity, is well accepted. Protection is vital, given the internet's crucial role in the provision of societal services across countries, and because severe disruption of this infrastructure could spur social, economic and political crises whose consequences could be far-reaching, long-term and serious. However, addressing the protection of critical infrastructure in general, let alone that specifically related to the internet, and its governance at the global level, is a complicated task. A key reason for this is that countries differ significantly in what infrastructure they consider to be critical.[3] This has traditionally been translated into a national prerogative in diplomatic negotiations, whereby states define nationally what they consider to be critical infrastructure. Despite this ambiguity, states have constructively discussed critical infrastructures in the GGE and the Open Ended Working Group (OEWG), underlining their importance, while respecting national understandings of criticality by not going into specifics. The implicit introduction

[1] United Nations General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* ('UN GGE Report'), 14 July 2021, A/76/135, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[2] Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015), https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

[3] OECD, *OECD Reviews of Risk Management Policies Good Governance for Critical Infrastructure Resilience* (Paris: OECD Publishing, 2019), https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en

of the notion of *transnational* CII arguably puts pressure on this diplomatic consensus, as it requires a shared international understanding of this infrastructure.

The recognition of the infrastructure underpinning the internet as critical by the 2021 GGE report is an important step forward in considering its potential governance at the international level. To progress thinking on this topic, *EU Cyber Direct* convened a group of 14 experts for a research seminar under the Chatham House Rule in The Hague in May 2023. The participants included academic experts and cyber diplomats as well as professionals from both industry and the technical community.[4] The aim of the seminar was to consider the global governance of the internet's infrastructure, using subsea cables and Internet Exchange Points (IXPs) as case studies, to focus the conversation. This paper is the product of that research seminar.

The paper first considers what is meant by transnational CII, outlining both its technical and political parameters. The second section advances the argument that infrastructure that is *critical* is not necessarily *vulnerable*, using IXPs as an example. Finally, considering subsea cables, the third section emphasises that states must strategically consider geopoliticisation and any resulting technical–political tensions when approaching the international governance of this type of infrastructure, noting that there is no one-size-fits-all approach. By way of conclusion a suggestion is offered for a model of meetings through which diplomats could structure advanced international discussions on topics such as transnational CII, in a concentrated and inclusive manner, under the Programme of Action (PoA) that is currently under discussion in the OEWG.

[4] Participants were: Arjen Boin (Leiden University), Chris Buckridge (RIPE NCC), Madeline Carr (University College London), Antonio Coco (University of Essex), Marie Humeau (Mission of the Netherlands to the UN), Camino Kavanagh (King's College London), Konstantinos Komaitis (Lisbon Council), Triantafyllos Kouloufakos (LU Leuven), Manon Le Blanc (European External Action Service), Tobias Liebetrau (University of Copenhagen), Nikolas Ott (Microsoft), Jesse Sowell (University College London), Paul Timmers (University of Oxford) and Bill Woodcock (Packet Clearing House).

What do we talk about when we talk about transnational critical information infrastructure?[5]

The need to protect transnational CII was highlighted in the 2021 reports of both the UN GGE and OEWG on cybersecurity – both of which were adopted by consensus.[6] In the OEWG report, states agreed 'on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, *along with endeavouring to ensure the general availability and integrity of the Internet*' (emphasis added).[7] The UN GGE report implied that some of such infrastructure is transnational, and as such goes beyond the protection of national critical infrastructure, and some is national but is vital for providing 'services across several States such as the technical infrastructure essential to the general availability or integrity of the internet'.[8]

These UN formulations were built on the concept of the protection of the public core of the internet, originally coined in 2015 by Dennis Broeders at the Netherlands' Scientific Council for Government Policy.[9] The public core norm was originally formulated as a negative norm of restraint for states. The aim of the norm was to protect the internet as a global public good, by establishing and disseminating an international standard stipulating that the internet's public core – its main protocols and infrastructure – must be safeguarded against unwarranted intervention by governments.[10] The public core concept includes (a) logical and technical infrastructure that is in essence transnational – like the core protocols of the internet, which are not meaningfully territorial in any sense, and the cable infrastructure connecting the continents – as well as (b) infrastructure that is 'national' in a territorial sense, but underpins the regional or global provision of services through the internet, like IXPs and cable landing stations. Since 2015 the concept has been further developed in multi-stakeholder fora as well as in government policy documents.

---

[5] The first part of this section builds on Dennis Broeders and Arun Sukumar, 'Core Concerns: the Need for a Governance Framework to Protect Global Internet Infrastructure', *Policy and Internet* (2023), https://doi.org/10.1002/poi3.382, accepted for publication.

[6] United Nations General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, Final Substantive Report ('OEWG Report'), 10 March 2021, A/AC.290/2021/CRP.2; UN GGE Report.

[7] OEWG Report, B.26. For an in-depth analysis of the OEWG and GGE processes and the public core, see Dennis Broeders, 'The (Im)possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: a Mid-process Assessment', *Journal of Cyber Policy* 6 (2021), 277–297.

[8] UN GGE Report, p. 46.

[9] Broeders, *The Public Core of the Internet.*

[10] Ibid.

The Netherlands addressed the protection of the public core of the internet in its 2017 *International Cyber Strategy*[11] and in the same year, the multi-stakeholder Global Commission on the Stability of Cyberspace (GCSC) proposed a norm on the issue in its final report.[12] Through the norm, the GCSC called on state and non-state actors to 'neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the internet, and therefore the stability of cyberspace'.[13] The formulation 'intentional and substantial damage' to the public core acknowledges that many states will allow military and intelligence operations that (mis)use public core protocols and infrastructure, but should stop short of causing substantial damage with intended or unintended transnational effects.

Since 2017, this norm has found wide support from states and other actors. In 2018, it was taken up in the *Paris Call for Trust and Security in Cyberspace*, a multi-stakeholder initiative championed by the French government.[14] While non-binding, the Paris Call has been endorsed by over 80 states, with the United States joining in November 2021. The 'public core' concept has also become part of EU policy, for example in the EU Cyber Security Act, which gives the European Union Agency for Cybersecurity the responsibility to 'support the security of the public core of the open internet and the stability of its functioning'.[15] In 2022, the European Union updated the Network and Information Systems Directive (NIS 2), reiterating its support for the protection of the public core and underlining the cross-border nature of both critical infrastructure and cyberattacks.[16]

Technical parameters

The infrastructure that 'provides services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet', being built

[11] Government of the Netherlands, *Building Digital Bridges: International Cyber Strategy: Towards an Integrated International Cyber Policy* (2017); see also the new Dutch international strategy: Government of the Netherlands, *International Cyber Strategy 2023–2028. Decisive Diplomacy in the Digital Domain* (2023),
https://www.government.nl/documents/publications/2023/09/12/international-cyber-strategy-netherlands-2023-2028

[12] GCSC, 'Call to Protect the Public Core of the Internet' (2017), https://hcss.nl/wp-content/uploads/2022/08/call-to-protect-the-public-core-of-the-internet.pdf

[13] GCSC, 'Definition of the Public Core, to Which the Norm Applies' (2017: 21), https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf

[14] Ministère de l'Europe et des Affaires étrangères, 'Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace', *France Diplomacy* (2021), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[15] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade: Joint Communication to the European Parliament and the Council by the High Representative of the Union for Foreign*
Affairs and Security Policy, JOIN (2020) 18 final, 151/19, 151/35.

[16] *Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common level of Cybersecurity Across the Union*, 14 December 2022 (NIS 2 Directive).

on the notion of the public core of the internet, includes the internet's core logical and technical infrastructure and, to some extent, the organisations that supply and administer these.[17] The internet's core has fuzzy edges as it is not always immediately clear what is essential to the internet's availability and integrity. Moreover, this can change as the global network develops and evolves. Core internet protocols such as TCP/IP, BGP and DNS and core technological infrastructure such as subsea cables and landing stations, DNS servers and internet exchanges are generally considered as part of the core. In 2018, the GCSC published a paper on the interpretation of the public core, outlining four technical elements: 'The norm identifies four broad elements of the public core: (1) the packet routing and forwarding elements, (2) the naming and numbering systems, (3) the cryptographic mechanisms of security and identity, and (4) the physical transmission media.'[18] Policy actors, such as the EU, have at times also highlighted specific elements of the public core that merit protection and attention. In the 2019 Cyber Security Act, the EU highlighted 'key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone'.[19] In the NIS 2 Directive of 2022, the EU promotes policies 'related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables'.[20] In the wake of Russia's war in Ukraine and the sabotage of the Nord Stream 2 pipeline, there has been increased (political) attention on undersea infrastructure.[21]

Political parameters

Politically, the vulnerability and the need for protecting the public core of the internet and transnational CII are firmly embedded in the UN discussions on the framework for responsible state behaviour in cyberspace. As these discussions take place within the First Committee of the UN, the issue is set in the context of international security and stability. This has consequences for these discussions, as it sets a premium on thinking about transnational infrastructure and service provision primarily as a security issue, directing thinking towards vulnerabilities and malicious actors. The protection of transnational CII has been made part of the norms on infrastructure protection that were originally

[17] See Dennis Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security', *Journal of Cyber Policy* 2 (3) (2017), 366–376; Broeders, 'The (Im)possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG'.

[18] GCSC, 'Definition of the Public Core, to Which the Norm Applies'.

[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[20] NIS 2 Directive.

[21] Camino Kavanagh, *Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour* (Geneva, Switzerland: UNIDIR, 2023), https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf

formulated in the 2015 UN GGE report[22] and that were given an 'added layer of understanding' in the 2021 consensus report. That makes the protection of transnational CII first and foremost a *negative* norm of restraint for states – taking it off the table for (peacetime) cyber operations. However, transnational CII is also vulnerable to safety concerns (i.e. disruptions without malicious intent), which are mostly outside the scope of thinking in the UN First Committee but may be equally dangerous. The global technical community, the companies that create and operate infrastructure and in some cases the international computer security incident response team (CSIRT) community are the first responders for many of the safety crises on the global internet. But, given the importance of transitional CII, it is worth asking whether states also have *positive* obligations to provide protection that could be part of the deliberations in the First Committee.

[22] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 20152, A/70/174 (22 July 2015, https://digitallibrary.un.org/record/799853).

Critical infrastructure is not necessarily vulnerable

The classic definition of a risk is the *impact* of an event multiplied by the *chance* of that event actually taking place. Nuclear disaster is considered high-risk, but mostly on account of its devastating impact rather than on the chance of it actually occurring. However, when impact and chance are combined, it still poses a significant risk. Political concern about transnational CII is more evenly spread between chance and impact. The core logical and technical infrastructure were not originally built with security in mind, and core protocols such as BGP and the DNS system are vulnerable to tampering. When they are attacked or misused, the scale of the effects is often transnational. While we have not seen attacks that deliberately target core infrastructure or use core protocols for a destructive attack, lesser evils such as BGP hijacking, DNS blocking and, more recently, attacks on CII infrastructure in Ukraine have been experienced in real life. Subsea cables function as the central nervous system of the global internet, but are, for most of their trajectory between continents, protected from human damage or disruption only by the fact that they lie on the seabed or ocean floor. And yet, political uneasiness about the vulnerability of subsea cables is rising as suspicions mount about Russian capabilities and political will to interfere with them. An increase in the chance of it happening – real or imagined – raises the perceived risk.

If 'critical' in transnational CII is (1) something that is *vital* for the functioning and provision of the global internet and (2) something that is potentially *vulnerable* to external shocks, either intentional (security) or unintentional (safety), then we have a variation in risks and possibly in the mitigation of those risks. There can be vital infrastructures that are vulnerable and vital infrastructures that are less vulnerable, or, indeed, not vulnerable at all. Some vulnerabilities are the result of state behaviour; some of corporate, market-driven behaviour; some of commercial activities; and others still of environmental factors. Some solutions can be provided by states and some by the private sector, and some require a mix of the two.

In risk mitigation, there are matters that are primarily in the hands of states, which can be formulated as negative obligations (in the first place, adherence to the norm of restraint) or as positive obligations (creating opportunities for resilience and preventing market failures). Important parts of risk mitigation are in the hands of private parties and/or the technical community. In the background, private companies and critical infrastructure operators continuously work on improving the functioning of the internet as a system of systems. This is the normal state of affairs of distributed, global network management, but it includes considerations of optimising technology and the network,

as well as business interests. These often align, but they can also clash.[23] The best solution is not always the cheapest solution.

Public and private actors also follow different logics. Whereas policymakers, especially those working on (national) security, tend to think in terms of offence and defence and/or crime and punishment, the technical community tends to think in terms of technical solutions such as the redundancy of systems. For example, the risk of BGP hijacking – a great worry for states – is in part addressed by the technical community through the development of BGP RKPI: a technical, cryptographic solution to a technical and political problem. In other words, threat mitigation, even of security threats, can require private technological solutions as well as government solutions. However, assigning and arranging public and private responsibilities is not always easy. Even though most countries have structures and procedures in place for critical infrastructure protection that assign responsibilities to private and public parties, these do not translate naturally into a model for the protection of transnational infrastructure that involves multiple companies and countries.

Internet Exchange Points

IXPs, which were discussed as a CII during the research seminar, are an interesting illustration of these public–private dynamics, in terms of vulnerability and risk mitigation. The internet constitutes a network of networks, and IXPs are physical facilities that enable internet service providers (ISPs) – the networks – to exchange internet traffic between them.[24] Today, at least 751 IXPs are located around the world, hosted by 159 countries.[25] The number of IXPs housed by any given country varies, from the US hosting as many as 122 to some countries having none at all.[26] IXPs can comprise either informal projects or formally incorporated entities, where trust, cooperation, financial management and transparent governance models are essential, as they constitute an arrangement among often competing networks.[27] The location of IXPs matters in terms of financial efficiency, service performance and the willingness of networks to participate, and are best hosted in a neutral space to encourage participation.[28] 'In the regions where IXPs are densest

[23] Madeline Carr, 'Public–Private Partnerships in National Cyber-security Strategies', *International Affairs* 92(1) (2016), 43–62, https://doi.org/10.1111/1468-2346.12504

[24] Bill Woodcock and Benjamin Edelman, *Toward Efficiencies in Canadian Internet Traffic Exchange* (Ottawa: Canadian Internet Registration Authority, 2012), https://courses.acs.uwinnipeg.ca/3907-050/Course2020/Toward-Efficiencies-in-Canadian-Internet-Traffic-Exchange2.pdf

[25] Packet Clearing House, 'Packet Clearing House Report on Internet Exchange Point Locations' (2023), https://www.pch.net/ixp/summary#!mt-zoom=%5B1.6200069472640912%2C-0.19504506035757319%2C-0.38271869655323065%5D

[26] Ibid.

[27] Woodcock and Edelman, *Toward Efficiencies in Canadian Internet Traffic Exchange*.

[28] Ibid.

and most common, networks enjoy the highest levels of growth and profitability, and consumers' internet access tends to be particularly fast and inexpensive.'[29] While IXPs are generally robust entities, they can, for example, be threatened in their operation by natural phenomena (such as earthquakes, fires, natural disasters and climate change in the form of sea-level rise), human error, technical faults, power outages and deliberate attacks.[30] IXPs are critical to the functioning of the global internet in the sense of being technically vital. But a second question is whether they are vulnerable, which deserves a much more nuanced answer.

The general rule with IXPs seems to be that the best answer to security threats and safety risks is increased redundancy. More is more, and less constitutes a risk. This becomes clear when we compare Estonia and Georgia – two countries that have suffered digital attacks at the hands of Russia. The 2007 distributed denial-of-service (DDoS) attacks on Estonia targeted internet infrastructure as well as defacing websites. In response to this attack, 'a redundant pair of IXPs in Tallinn formed the linchpin of the Estonian defense', as the country received fast and effective aid from ISPs located in several diplomatically friendly neighbouring states.[31] With this redundancy offering international connectivity, Estonian vulnerability was curbed as the country maintained its capacity to navigate the attack, which ultimately 'amounted to little more than a nuisance'.[32] Since the attack, Estonia's internet resilience and redundancy have been enhanced with the establishment of additional IXPs. Based on location within Estonia, the country now has three IXPs (RTIX, PITER-IX and IIX). If we consider organisation, a fourth IXP (BALT-IX) can be added to this count: although based in Vilnius, it has connections with data centres in Tallinn. Of these, only RTIX was created, and is now operated, by the public sector.

In 2008, Georgia suffered a cyberattack, which coincided with the Russian army invading its territory. As had been the case in Estonia, this attack was characterised by DDoS attacks and website defacements.[33] Georgia was, however, not as well placed to respond

---

[29] Ibid.

[30] Jorik Oostenbrink and Fernando Kuipers, 'A Global Study of the Risk of Earthquakes to IXPs', in *Proceedings of the 2022 IFIP Networking Conference (IFIP Networking)* (Catania, Italy: IEEE, 2022), https://research.tudelft.nl/en/publications/a-global-study-of-the-risk-of-earthquakes-to-ixps; Holly Gittins, '"Extensive' damage after fire breaks out at internet exchange in Hemsworth', *Wakefield Express*, 22 March 2021, https://www.wakefieldexpress.co.uk/news/extensive-damage-after-fire-breaks-out-at-internet-exchange-in-hemsworth-3173587; Christoph Dietzel, 'Improving Security and Resilience Capabilities of the Internet Infrastructure' (MSc diss., Technische Universität Berlin, 2019), https://www.researchgate.net/publication/337919072_Improving_Security_and_Resilience_Capabilities_of_the_Internet_Infrastructure#fullTextFileContent; Ramakrishnan Durairajan, Carol Barford and Paul Barford, 'Lights Out: Climate Change Risk to Internet Infrastructure', *Proceedings of the Applied Networking Research Workshop* (2018), https://ix.cs.uoregon.edu/~ram/papers/ANRW-2018.pdf; Alex Henthorn-Iwane, 'Understanding Internet Exchanges via the DE-CIX Outage', *Thousand Eyes*, 13 April 2018, https://www.thousandeyes.com/blog/network-monitoring-de-cix-outage; 'Outage at Amsterdam Internet Hub Affects Much of Netherlands', *NNL Times*, 13 May 2015, https://nltimes.nl/2015/05/13/outage-amsterdam-internet-hub-affects-much-netherlands

[31] Ross Stapleton-Gray and William Woodcock, 'National Internet Defense – Small States on the Skirmish Line', *Communications of the ACM* 54 (3) (2011), https://dl.acm.org/doi/pdf/10.1145/1897852.1897869

[32] Ibid.

[33] Paulo Shakarian, 'The 2008 Russian Cyber-Campaign Against Georgia', *Military Review*, November–December 2011, https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia

to the attack, one of its 'crippling deficiencies'[34] being its lack of an IXP. At the time, most of Georgia's internet traffic was routed through Russia, and its extremely limited international connectivity was a significant factor in how affected the country was by the attack.[35] Since then, it should be noted that three IXPs – all run by the private sector – have been established in Georgia, increasing the country's internet redundancy and resilience.[36]

Russia's war on Ukraine also highlights the 'more is better' principle with IXPs. Despite multiple disruptions as a result of Russia's invasion, Ukrainian networks have managed to retain their resilience, in part due to the country's large number of IXPs and widespread international connectivity.[37]

Redundancy comes from connectivity and the possibility to route around problems – whether they are intentional or unintentional. Countries without IXPs are vulnerable, especially if they cannot rely on their neighbours, and countries with a single IXP are vulnerable as that IXP may become a single point of failure. The bigger and more central an IXP is, the greater the chances of transnational effects should it go down. As with much critical infrastructure, IXPs are first and foremost businesses making commercial decisions. But on account of their being designated 'critical,' governments do get a say in some aspects of their business operations. Government policy has to accommodate both commercial interests and national security interests. In this respect countries are making very different choices.

When market consolidation in Estonia resulted in one IXP, the Estonian government decided to publicly fund a second, to make sure that there was not a single point of failure.[38] IXPs are vital irrespective of policy, but national policy can make a huge difference in terms of vulnerability. Creating the circumstances for, or actively promoting, redundancy by preventing monopolies creates stability in the system. For example, Brazil has a network of publicly funded IXPs that are part of an overarching project called IX.br. This is a non-profit business model managed and fully funded by NIC.br, the Brazilian Internet Steering Committee that takes care of DNS registry services and IP allocation, in addition to government-funded internet development activities.[39]

Vulnerabilities in the IXP ecosystem occur when there is a scarcity of IXPs in a country or a region. Sometimes redundancy is the result of market forces (for example, in the USA) and sometimes it is the result of public policy (such as in the Brazilian case). Transnational

[34] Stapleton-Gray and Woodcock. 'National Internet Defense'.

[35] Ibid.

[36] 'Packet Clearing House Report on Internet Exchange Point Locations.'

[37] João Tomé, David Belson and Kristin Berdan, 'One Year of War in Ukraine: Internet Trends, Attacks, and Resilience' (23 February 2023), https://blog.cloudflare.com/one-year-of-war-in-ukraine/

[38] Input by one of the seminar's participants.

[39] Samuel Henrique Bucke Brito, Mateus Augusto Silva Santos, Ramon Fontes and Danny Lachos Perez, 'Dissecting the Largest National Ecosystem of Public Internet eXchange Points in Brazil', *Conference: Passive and Active Network Measurement (PAM)*, 2016, https://link.springer.com/chapter/10.1007/978-3-319-30505-9_25

vulnerabilities in the IXP system would first need to be identified (through technical analysis) and addressed through national policy, investment and/or capacity-building efforts. There is no blanket solution.

Geopoliticisation and the global governance of critical information infrastructure

While redundancy in CII is increasing, so too are concerns about security. For this reason, it is essential that states strategically account for the geopolitical context when considering the (potential) global governance of this type of infrastructure, avoiding the creation of unnecessary inter-state tensions. On the one hand, states should work to ensure that the operation of CII is not unnecessarily politicised and policed by states. Governments should be cautious of securitising individual CII operational processes, which are often best left in the hands of the private and technical communities. Governments should also be mindful of international organisations with related pre-existing mandates in the area, to avoid the duplication or clashing of efforts. On the other hand, states must not be naïve, and where state intervention is determined to be necessary (for example, economically, militarily or politically), states must navigate the tension between technical and political solutions to protect their national and/or regional interests. Ultimately, states should aim to create and adopt transparent and system-appropriate governance mechanisms, which account for regional variation as well as fostering strategic autonomy, and that are based on the circumstances of any particular CII. There is no one-size-fits-all approach for governing diverse forms of CII.

Subsea cables

Subsea cables offer an interesting example of a CII that is facing a complex web of threats, and whose protection is becoming increasingly relevant to national security.[40] At present the subsea cable regime 'is made up of a patchwork of international treaties, regulatory frameworks, international and regional organisations, industry associations, protocols, standards and best practices'.[41] The 1982 United Nations Convention on the Law of the Sea (UNCLOS) is the international point of reference for states, and the International Cable Protection Committee (ICPC) is one of the main subsea cable bodies, 'where owners, operators and suppliers of subsea telecommunications or power cables and government representatives share technical, legal and environmental information'. Although the ICPC 'promotes awareness of … [subsea] cables as critical infrastructure,

[40] See, for example, Christian Bueger and Tobias Liebetrau, 'Protecting Hidden Infrastructure: the Security Politics of the Global Submarine Data Cable Network', *Contemporary Security Policy* 42 (3) (2021), https://www.tandfonline.com/doi/full/10.1080/13523260.2021.1907129; Hilary McGeachy, 'The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns', *Australian Journal of International Affairs* 76 (2) (2022), https://www.tandfonline.com/doi/full/10.1080/10357718.2022.2051427

[41] Kavanagh, *Wading Murky Waters*.

issuing best practices for cable protection and resilience, provides guidance on technical and regulatory issues and recommendations for cable installation, protection and maintenance', government participation, while welcomed, remains minimal.[42] In parallel, states are making moves to securitise this infrastructure, as is exemplified by the actions of a few states.

For example, in response to the 2022 sabotage of the Nord Stream pipelines, NATO allies have 'significantly increased their military presence around key infrastructure, including with ships and patrol aircraft' as well as setting up 'a Critical Undersea Infrastructure Coordination Cell at NATO Headquarters' with the intention of improving the security of highly vulnerable subsea cables and pipelines.[43] The US in its own right has also taken action fostering the securitisation of subsea cables. For instance, in 2022 the US urged its Federal Communications Commission to deny the building of a subsea cable connecting it to Cuba due to national security fears as the cable would be controlled by a Cuban state-owned telecommunications monopoly.[44] The US also rejected the development of four cables owned by Amazon, Meta and Google that would have connected it to Hong Kong, due to concerns over potential Chinese espionage.[45] China too has cited national security concerns in its slow granting or denial of permits allowing new cable projects to pass through the South China Sea.[46] Furthermore, several US administrations have managed to exclude China from the global subsea cable market. However, China has subsequently adapted by constructing its own cables as well as those of its allies, sparking fears of the subsea cable network being divided into eastern and western blocs.[47]

These examples of state actions vis-à-vis subsea cable development demonstrate a proactive tendency on the part of several major powers to de-risk, highlighting a particular technical versus political tension. Earlier, in the case of IXPs, it was determined that the more such entities there are, the better the situation is, in terms of ensuring redundancy and boosting internet resilience. Developing IXP infrastructure is a decision that is predominantly technical, characterised by relatively little political tension. This is not the case, however, with subsea cables. While redundancy in CII is highly prized, and the more subsea cables there are connecting regions, the greater the level of internet

---

[42] Ibid.

[43] NATO, 'NATO Stands up Undersea Infrastructure Coordination Cell', 15 February 2023, https://www.nato.int/cps/en/natohq/news_211919.htm; Julian Borger, 'Nord Stream Attacks Highlight Vulnerability of Undersea Pipelines in West', *The Guardian*, 29 September 2022, https://www.theguardian.com/business/2022/sep/29/nord-stream-attacks-highlight-vulnerability-undersea-pipelines-west

[44] David Shepardson, 'U.S. Urges Rejection of Undersea Cable Connection to Cuba', *Reuters*, 30 November 2022, https://www.reuters.com/world/americas/us-urges-rejection-undersea-cable-connection-cuba-2022-11-30/

[45] Elisabeth Braw, 'Decoupling Is Already Happening – Under the Sea', *Foreign Policy*, 24 May 2023, https://foreignpolicy.com/2023/05/24/china-subsea-cables-internet-decoupling-biden/

[46] Tsubasa Suruga, 'Asia's Internet Cable Projects Delayed by South China Sea Tensions', *Nikkei Asia*, 19 May 2023, https://asia.nikkei.com/Business/Business-Spotlight/Asia-s-internet-cable-projects-delayed-by-South-China-Sea-tensions

[47] Anna Gross, Alexandra Heal, Chris Campbell, Dan Clark, Ian Bott and Irene de la Torre Arenas, 'How the US Is Pushing China out of the Internet's Plumbing', *Financial Times*, 13 June 2023, https://ig.ft.com/subsea-cables/

resilience there will be between them, the examples above highlight that the 'more the merrier' approach is not always the determining driver. Instead, political risk calculations interact with the development of potential submarine redundancy capacity. Being connected to adversaries and enabling a potential avenue of espionage has ruled out the building of particular subsea cable projects – under certain consortia and between particular countries – in favour of political safety. Given the expanding subsea cable market (whose revenue is estimated to grow from US$17.18 billion in 2023 to US$41.02 billion in 2032) and the diversification of players within it, states will increasingly need to craft strategies for determining the relevance of particular projects to their economic, political and national security, and thus the level of attention they warrant.[48]

This tendency towards securitisation demands special attention because of the status of subsea cables as the central nervous system of the global internet. In specific relation to the EU's connectivity and security, these cables are paramount, as the vast majority of intercontinental data are transported via this infrastructure.[49] While 'Damage to a single cable would have minimal impact on network performance due to the availability of other paths', the system as a whole is vital as 'satellite networks do not have the bandwidth to replace what cables provide' and 'terrestrial options [are also not] a viable back-up option for all of Europe's interregional capacity'.[50] The EU's approach to the transnational governance of this infrastructure is not, however, indicative of the key role it actually plays with respect to the region's national, political and economic security as well as in ensuring its overall strategic autonomy. 'EU institutions have so far not laid out a policy, strategy, initiative or programme that would primarily and explicitly concern data cable protection.'[51] Subsea cables are touched on in various EU policy areas – including maritime security, cybersecurity policy, ocean governance, digital and infrastructure policy, and external action.[52] Moreover, individual EU member states have implemented their own arrangements in relation to the governance of this infrastructure through national-security-driven approaches (e.g. France and Portugal), civilian-steered initiatives (e.g. Malta) and industry-led self-regulatory arrangements (e.g. Denmark).[53] However, considering these initiatives, the EU's approach to the protection and governance of subsea cables overall has been found to be lagging behind and in need of improvement

[48] 'Submarine Cable System Industry Is Expanding at a Higher Pace', Precedence Research, 9 May 2023, https://www.precedenceresearch.com/press-release/submarine-cable-system-market; Kavanagh, *Wading Murky Waters*.

[49] Alan Mauldin, 'Cutting off Europe? A Look at How the Continent Connects to the World', *TeleGeography*, 13 October 2022, https://blog.telegeography.com/cutting-off-europe-a-look-at-how-the-continent-connects-to-the-world

[50] Ibid.

[51] Christian Bueger, Tobias Liebetrau and Jonas Franken. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*, EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/12, (2022), https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[52] Ibid.

[53] Ibid.

in terms of addressing the vulnerabilities that European digital connectivity faces,[54] in spite of having international points of reference, such as UNCLOS and the ICPC.

Although all EU member states depend on subsea cables for their cross-continental internet traffic, it is important to note that not all are equally important when it comes to actually protecting and governing them.[55] Five EU member states are landlocked, docking no subsea cables, and a significant number serve only as minor cable connection points to the wider world.[56] Five EU countries do, however, play a vital role in the EU's digital connectivity: Denmark, France, Italy, Portugal and Spain.[57] Spain and Portugal are vital for Europe's connectivity to the South Atlantic region (Africa and South America). Italy and France are the primary territories for landing cables connecting the continent to Asia, and Denmark is a major cable gateway to North America.[58] France is an interesting case for the EU, as alongside the US and Japan, its companies dominate the supply and installation of subsea cables globally, significantly eclipsing even its Chinese counterparts.[59]

The implications of France's dominance as both a key docking state and a global supplier of subsea cables – both internally among EU member states and externally in relation to the wider world – remain unclear, and need to be assessed. For example, does the leading role of French companies in supplying and installing global subsea cables offer the EU an advantage in securing its own strategic autonomy? If so, can the interests of France and the EU be aligned, and how? How could, or should, the role of an EU member state industry factor into transnational governance considerations of this infrastructure on the EU's part (especially given that the most common financing model of subsea cable development has been that of consortiums, which may have a complex international character)?[60] Furthermore, this model is changing, with greater concentration in US hyperscalers likely having a downstream impact on the EU cable industry, affecting both small and large companies. The EU must also consider what the strategic importance of France's position in the subsea cable area means for its broader action on cyber issues.

Another vital element when one is considering the transnational governance of subsea cables is their landing stations. Landing stations 'house the "dry plant" infrastructure, which includes the submarine line terminal equipment that controls its operations, and the equipment that powers the cable'.[61] It is here that the transnational cable generally meets national infrastructure under the explicit jurisdiction of the country in which it is

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Gross et al., 'How the US is Pushing China out of the Internet's Plumbing'.

[60] Doug Brake, 'Submarine Cables: Critical Infrastructure for Global Communications', *Information Technology & Innovation Foundation*, April 2019, https://www2.itif.org/2019-submarine-cables.pdf

[61] Kavanagh, *Wading Murky Waters*.

situated. How landing stations feature in transnational governance approaches to subsea cables is important to establish, to ensure that roles, responsibilities and rights are clearly defined. States will need to determine what the international standing of landing stations is, given their positioning at the national/international nexus. States will have to work with relevant stakeholders to evaluate who is best placed to protect these stations (for example, states, the private sector or the technical community) and respond to transnational incidents to ensure continuous operation. While much of this is covered through national legislation and permitting and licensing decisions, securitisation plays a role here too. Here again the tension of technical versus political solutions arises: making the decision to connect a subsea cable to any particular landing station is not just a technical calculation, but one that has to account for political trust. As landing stations are entities within sovereign territories, they are, in effect, extensions of their respective states. So determining whether or not to connect a subsea cable to any given landing station becomes a matter of the state of relations and the level of trust enjoyed among the states to be potentially connected. Questions of de-risking and strategic autonomy will weigh heavily here, and connecting subsea cables to specific landing stations will not simply be a matter of enhancing access and redundancy in the submarine network.

Assessing the configuration of landing stations, as well as designing a fit-for-purpose transnational approach to the governance of subsea cables, will also depend on (a joint) understanding of the risks and threats. While case studies detailing the disruption, damage or total destruction of subsea cables are scarce in the literature, recently published studies have highlighted just how extensive the threats *potentially* facing this infrastructure are.[62] These threats can be intentionally or unintentionally realised, and can be categorised as natural, geographic, commercial, technical, digital, cyber, economic, criminal and political in nature.[63] Some threats are more relevant in certain regions, highlighting the need for governance mechanisms that are context-sensitive. For instance, some cables lie in areas more prone to natural disasters. In 2006, for example, nine subsea cables were damaged by an earthquake near Taiwan, which resulted in China, Taiwan, Vietnam, Japan, Singapore and the Philippines losing critical communication

[62] Ibid.; Bueger et al., *Security Threats to Undersea Communications Cables and Infrastructure.*

[63] For more detailed examples of these risks, see for example Bueger et al., *Security Threats to Undersea Communications Cables and Infrastructure*; Kavanagh. *Wading Murky Waters*; Christian Bueger and Tobias Liebetrau, 'Protecting Hidden Infrastructure: the Security Politics of the Global Submarine Data Cable Network', *Contemporary Security Policy* 42 (3), 2021, https://www.tandfonline.com/doi/full/10.1080/13523260.2021.1907129; Himmat Singh Sandhu and Siddhartha Raja, 'No Broken Link: the Vulnerability of Telecommunication Infrastructure to Natural Hazards', *World Bank Group* (2019), https://documents1.worldbank.org/curated/en/951991560791754833/pdf/No-Broken-Link-The-Vulnerability-of-Telecommunication-Infrastructure-to-Natural-Hazards.pdf; Simon Scarr, Wen Foo, Vijdan Mohammad Kawoosa, Anand Katakam and Aditi Bhandari. 'The Race to Reconnect Tonga', *Reuters*, 28 January 2022, https://www.reuters.com/graphics/TONGA-VOLCANO/znpnejbjovl/; Sydney Brooke Pleasic, 'Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally', Student Works, Seton Hall Law (2024), https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2438&context=student_scholarship; Jamie Taraby, 'An Underwater Hack and the Digital Ripple Effects', *Bloomberg*, 20 April 2022, https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects

links, and disruption of regional trade, banking and markets.[64] To offer another example, some subsea cables are concentrated in bottlenecks or choke points, including along major commercial routes, as is the case in Egypt, where 16 cables (carrying an estimated 17% of the world's internet traffic) connecting Europe to the Middle East, East Africa and Asia pass through its territory.[65] Several incidents involving subsea cables have already been reported in this area.[66] Overall, regional assessments will need to be continuously carried out to understand the key threats to connectivity via subsea cables in different areas of the world. Some of these assessments are already standard practice, but are not necessarily connected to the debates about cybersecurity and the geopoliticisation of critical infrastructure.

When one considers subsea cables, especially relative to the earlier discussion of IXPs, it becomes clear that the governance of CII must be infrastructure-specific. The fact that both are crucial parts of transnational CII – and should be recognised as such – does not mean that their protection requires the same prescription. While 'more is more' in the case of IXPs, a much deeper political calculation is required for the development of the subsea cable network. What is possible and makes sense technically may not be (or be perceived to be) best geopolitically. Hence when it comes to initially contemplating and later designing a global governance regime, critical and careful consideration needs to be given to how technical needs and logic are weighted against political realities and relationships. Furthermore, states must remember that while they certainly have to understand the operation of CII relevant to their national security, their intervention may not always be for the best. Rather, certain infrastructural systems will function better in the hands of the technical community and private sector already running them.

[64] 'Underseas Cables Are the Lifeline for the Global Internet Economy and Depend on Legal Protection', *Unclosdebate*, 'Arguments', https://www.unclosdebate.org/argument/861/underseas-cables-are-vital-global-economy#:~:text=Modern%20fiber%20optic%20cables%20are,States%2C%20and%20indeed%20the%20world

[65] Sebastian Moss, 'Egypt's Submarine Cable Stranglehold', *DCD*, 15 September 2022, https://www.datacenterdynamics.com/en/analysis/egypts-submarine-cable-stranglehold/; Bueger et al., *Security Threats to Undersea Communications Cables and Infrastructure*.

[66] See for example Matt Burgess, 'Why Egypt Became One of the Biggest Chokepoints for Internet Cables', *arsTechnica*, 11 March 2022, https://arstechnica.com/information-technology/2022/11/the-most-vulnerable-place-on-the-internet/?comments=1&comments-page=1; 'Egypt Arrests as Undersea Internet Cable Cut off Alexandria', *BBC News*, 27 March 2013, https://www.bbc.com/news/world-middle-east-21963100; Bobbie Johnson, 'How One Clumsy Ship Cut off the Web for 75 Million People', *The Guardian*, 1 February 2008, https://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet

Conclusion

The governance of transnational CII will become increasingly relevant, and discussions in the area must continue. By way of conclusion, it is suggested here that diplomats structure advanced international discussions on transnational CII, in a concentrated and inclusive manner, under the Programme of Action (PoA) currently being developed in the OEWG.

A PoA is 'an outline, or programme, of practical actions that endorsing parties agree to implement as a way to achieve stated shared objectives'.[67] In the first annual progress report of the ongoing OEWG, one of the recommended next steps was for states to 'engage in focused discussions, on the relationships between the PoA and the OEWG, and on the scope, content and structure of a PoA'.[68] This paper offers a suggestion for a model of meetings that can be hosted under the auspices of the PoA, which the European External Action Service (EEAS) can propose to the OEWG.

This model of meetings could emulate the format of the research seminars that *EU Cyber Direct* has successfully hosted over the past few years to engage with experts. As part of the PoA, a series of seminars involving diplomats and technical specialists can be convened to focus on key topics of the discussions to help inform understandings in the broader negotiations. Discussing the global governance of transnational CII, and related questions about vitality and vulnerability, could help states to focus on the most vulnerable parts of this shared infrastructure.

Convening such seminars would create an ongoing inter-regional, cross-disciplinary forum under the PoA, where topic-specific experts are brought in on a case-by-case basis to progress international thinking on concentrated issues that define the negotiations. Through this format, meaningful strategic partnerships as well as circles of trust can be built and expanded among, as well as between, states and a wide range of stakeholders, establishing new epistemic communities that can, through time, help develop the international cyber regime in a targeted manner. The PoA could schedule several seminars per year, to ensure that discussions on key issue areas continue, and progress between UN substantive sessions. In that sense the discussions about transnational CII could become a 'track' under the PoA. The EU has a track record of conveying expert sessions and engaging with the technical community. This places the EEAS in a good position to further shape and table this suggestion at the OEWG as well as to coordinate international efforts at making these meetings a success.

---

[67] Allison Pytlak, *Programming Action: Observations from Small Arms Control for Cyber Peace* (Geneva: Women's International League for Peace and Freedom, 2021), https://reachingcriticalwill.org/images/documents/Publications/cyber-poa.pdf

[68] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*. 8 August 2022. A/77/275. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement

About the authors

Lise H. Andersen is a Post-Doctoral Researcher in the EU Cyber Direct Program, based at the Institute of Security and Global Affairs at Leiden University. Prior to this, Lise undertook her PhD at University College London's Department of Science, Technology, Engineering and Public Policy. Broadly speaking, Lise's research interests focus on the management of knowledge informing multilateral diplomatic activity, specifically in the scientific and technological space. She holds an MSc in Global Governance and Diplomacy from the University of Oxford, and a BA in Global Studies from the University of California Santa Barbara.

Dennis Broeders is Full Professor of Global Security and Technology at the Institute of Security and Global Affairs (ISGA) of Leiden University, the Netherlands. He is the Senior Fellow of The Hague Program on International Cyber Security and project coordinator at the EU Cyber Direct Program. His research and teaching broadly focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance. He is the author of the book The public Core of the Internet (2015). He served as a member of the Dutch delegation to the UN Group of Governmental Experts on international information security and the Open Ended Working Group (2019-2021) as an academic advisor. Before joining Leiden University he was professor of Technology and Society at Erasmus University Rotterdam and senior researcher and project coordinator at the Netherlands Scientific Council for Government Policy, a think tank within the Dutch Prime Minister's office.

About EU Cyber Direct

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.