AESCON

POLICY BRIEF SERIES 02-2022

Michał Rekowski

SECURE AND RESILIENT DIGITAL INFRASTRUCTURE: AN AGENDA FOR EUROPE AND ASIA

AESCON Policy Brief Series editors: Maaike Okano-Heijmans and Brigitte Dekker

This study is funded by the European Union's Partnership Instrument

ABSTRACT

Digital connectivity serves as the foundation for the modern world, promising benefits of digital transformation in almost every aspect of social and individual life. However, the digital infrastructure underpinning digital connectivity is faced with a growing number of risks and challenges, from cyber-attacks to advancing geopolitical competition that is increasingly centred on technology and infrastructure. To reap fully the benefits of digital transformation, governments need to invest in trusted digital infrastructure that is both resilient and secure. Partners in Asia and Europe that broadly share norms and perspectives on security in the digital world could benefit from enhanced cooperation on joint projects aimed at strengthening the security and resilience of digital infrastructure, thus ensuring a more sustainable digital future for their societies. This AESCON Policy Brief assesses what principles these partners should follow to achieve shared objectives; why these are important; and what could be approaches to and the benefits of cooperation between (groups of) countries in both regions.[1]

INTRODUCTION

Digital connectivity – that is, the ability of societies and individuals to connect and exchange data via digital infrastructure – promises great benefits in all aspects of the economy and society. In 2020, the global number of internet users grew by over 10 per cent, which represented the largest increase in a decade, reaching 4.9 billion people in 2021. During the years 2020–2022, the coronavirus pandemic not only hastened the process of digitalization all over the world, but further contributed to an environment in which individuals, companies and governments that embrace digital technologies are more likely to succeed. The COVID-19 crisis has set both Asia and Europe at the forefront of the pandemic-driven augmentation of digital transformation when compared to other regions.[2] Expanding the adoption of digital technologies also provides a solid foundation for post-pandemic recovery in both regions. Digitalization not only effectively enables administrations, businesses and individuals throughout crises to adapt and sustain their operations or even upscale them to new levels, but also provides a base for a more innovation-driven economy, for example by raising a volume of generated data that can later be harnessed for improved public and commercial uses.

At the same time, the number and scope of risks and challenges to digital infrastructure have increased, with a growing number of cyber-attacks and geopolitical tensions threatening to weaponize connectivity and reinforce the disruptive aspects of digital transformation. As a result, digital infrastructure has become both a great enabler and a bottleneck of the global economy and international society. The need to develop trusted, secure and resilient digital infrastructure becomes a central requirement for securing our increasingly connected world and to reap fully the benefits of digital transformation. Democratic countries in Europe and Asia share some of the key challenges in this context and could benefit from joint initiatives and greater cooperation related to the development of trusted digital infrastructure. Together, they could build new foundations for a trusted global connectivity and fully establish themselves as the leaders of a more secure and responsible digital transformation. Such foundations should be centred on four crucial areas of collaboration: (1) policy coordination on key values and principles; (2) the joint development of standards and regulations; (3) adopting security-by-design as a guiding principle; and (4) providing economic opportunities. Drawing from the session on 'Secure,

1 AESCON, the Asia-Europe Sustainable Connectivity Scientific Conference, is an initiative funded by the European Union (EU) and supported by the Asia Europe Meeting (ASEM), to discuss about sustainable connectivity. It brings together policy analysts, government representatives, the private sector, and other stakeholders, with a particular focus on Asia-Europe connections. In March 2022 the conference was organized by a consortium of think tanks in Europe and Asia, consisting of the Clingendael Institute (The Hague), the Kosciuszko Institute (Kraków), Carnegie India (New Delhi), GIZ (Bonn) and the Institute for South Asian Studies (ISAS/NUS, Singapore).

2 L. LaBerge et al., How Covid-19 has pushed companies over the technology tipping point and transformed business forever, Survey, McKinsey & Company, 5 October 2020.

resilient and responsible digital infrastructure' at the 2nd edition of the Asia–Europe Sustainable Connectivity Conference (AESCON) held in March 2022, this AESCON Policy Brief addresses these challenges and offers actionable steps.

WHAT IS TRUSTED DIGITAL INFRASTRUCTURE?

Digital infrastructure denotes increasingly complex systems that comprise both physical components (such as fibre cables, radio towers, communication satellites and data storage hardware) as well as virtual (such as software, digital platforms and internet protocols). The first group is sometimes also referred to as *hard* infrastructure, as differentiated from *soft*[3] digital infrastructure, which includes novel digital services and applications (for example, fintech or e-administration), devices (such as Internet of Things devices) and even social institutions providing governance, maintenance or education.[4] Generally speaking, the purpose of hard digital infrastructure is to provide physical channels that enable connectivity, whereas the purposes of soft digital infrastructure are to manage, sustain and optimize it. With the increasing reliance of governments, societies and individuals on digital products and services, the importance also grows of ensuring the undisrupted availability and uncompromised integrity of such products and services. The more that digital technologies penetrate every aspect of our lives, the more confident we want to be that they will not fail us in crucial moments. From banking and labour to state–citizen relations and electoral processes, technology becomes ubiquitous. Thus, it becomes an essential challenge to ensure that digital infrastructure can be trusted with this increasingly critical role that it plays in the functioning of our societies.

Trust in digital infrastructure refers to an assumption that digital infrastructure (both hard and soft) will continue to deliver on its objective – to provide undisrupted connectivity that enables the digital transformation and empowers rather than constrains or endangers its participants. Therefore, only digital infrastructure that is secure and resilient can be trusted. Securing digital infrastructure means protecting its components from threats that aim to destroy, obstruct or exploit them to undesired ends. These may include attempts to tamper with infrastructure, for example by compromising the integrity of a device to gain unauthorized access or control over it, disrupt its operations or even permanently render it dysfunctional. Resilience in the context of digital infrastructure denotes the ability to maintain the functionality of an infrastructure despite the occurrence of such threats.[5] In other words, resilient infrastructure remains to serve its purpose despite being the target of attack or interference. Resilience may be characterized as comprising 'the ability to anticipate, withstand, recover from and adapt to adverse conditions'.[6] Ensuring the security and resilience of infrastructure is crucial for making it a trustworthy element of the digital transformation. Even temporal failures of connectivity may affect the continuity of businesses and the functioning of key services such as education, public services or health care. As a result, companies may lose clients, administrations may strive to deliver critical utilities, and even the health and life of individual people may be endangered if technological factors paralyze medical institutions.[7] Trust in digital technologies may also be eroded, further limiting chances to reap the benefits of digital transformation fully. As the 21st century economy will be defined by digital innovation, countries that fail to adapt and transform their economies accordingly will inevitably descend in the global value chain.

3 Digital Infrastructure Sector Strategy (Draft): AIIB's role in the growth of the digital economy of the 21st century, AIIB, 8 January 2020.

4 R. Kumar and N. Strazdins, 'The digital infrastructure divide in the Commonwealth', Commonwealth Secretariat, Trade Competitiveness Briefing Paper, January 2021.

5 P.W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014, p. 36.

6 'Cyber Resiliency FAQ', The MITRE Corporation, 2017.

7 This was the case in 2020, when a cyber-attack paralyzed the functioning of a hospital in Dusseldorf, Germany, indirectly causing the death of a patient who could not be admitted despite urgent need.

SHARED CHALLENGES IN THE DEVELOPMENT OF SECURE AND RESILIENT DIGITAL INFRASTRUCTURE

Democratic countries in both Europe and Asia share similar challenges in the context of the security and resilience of digital infrastructure. These include security threats, the evolving geopolitical environment and economic dilemmas. Of these, security threats are the most direct, and concern developments related to cyber-attacks and growing offensive activity by hostile states in cyberspace.

The security risks related to a growing global number of cyber-attacks have been particularly notorious in Europe and Asia.[8] According to IBM, Asia and Europe were the most targeted regions in the world in terms of cyber-attacks in 2021, with 26 per cent of all recorded attacks taking place against Asia and 24 per cent against Europe.[9] Both regions were similar in the types of attacks they experienced, with ransomware, server access attacks and data theft the most common. Japan, Australia, India, the United Kingdom, Italy and Germany were the most attacked countries in both regions. In addition, a substantial group of the most infamous persistent threat actors (called APTs in cyber-security jargon, an acronym for advanced persistent threats) primarily originates in countries located in Europe and Asia, such as Russia, Belarus, Iran, North Korea and China.[10] States like Russia and North Korea seem to consider offensive cyber operations as below the threshold of armed conflict,[11] which means that they might be more prone to exploit these methods since, in their perception, the potential costs they would have to bear because of retributive or punitive actions are low. This results in a greater incentive for politically motivated cyber-attacks on critical infrastructure, which have recently targeted South Korea,[12] Japan,[13] Germany[14] and Ukraine, among many other countries in Europe and Asia. Both regions currently function as hotbeds for geopolitical tensions between formidable powers – including in Eastern Europe, the Taiwan Strait, or the South and East China Seas. This factor, paired with the increase of state or state-sponsored hostile activity in cyberspace,[15] contributes to the emergence of a more dangerous cyber environment in Europe and Asia, where states feel more incentivized to use cyber weapons to pursue their geopolitical interests.

A second reason why secure and resilient digital infrastructure is of growing importance is that digital technologies in general are becoming an area of geopolitical competition, with a strong ideological component differentiating between democratic and authoritarian uses of technology.[16] The development of specific novel technologies such as quantum computing, 5G or artificial intelligence (AI) is being considered by decision-makers in China, the United States, Russia and, increasingly, also in Europe as a source of power that can be projected internationally. This rivalry over tech supremacy also underpins the field of global technology governance and technology standards-setting procedures. Such technologies are also becoming the target of malicious meddling themselves – for example, algorithms running AI can also be tampered with in order to disrupt or repurpose their functioning. The negative consequences of such interference, especially when undertaken for political or geopolitical reasons, are unknown. In addition, there are a growing

8 For an overview of the evolution of the cyber-threat landscape, see, for example, ENISA, 'ENISA threat landscape 2021', October 2021.

9 IBM Security, 'X-Force Threat Intelligence Index 2022', IBM Report, 2022.

10 '2022 Global Threat Report', Crowdstrike, 2022.

11 Patryk Pawlak et al., 'Cyber conflict uncoded: the EU and conflict prevention in cyberspace', EUISS, Conflict Series Brief 7, April 2020.

12 C. Glover, 'North Korea is ramping up cyberattacks on South Korean targets', Tech Monitor, 22 June 2021.

13 N. Goud, 'Cyber-attacks on Japan's critical infrastructure touches 128 billion mark', Cybersecurity Insiders.

14 I. Wrede 'German firms in the crosshairs of Russian hackers?', Deutsche Welle, 25 March 2022.

15 This point was stressed during the panel at AESCON by Cameron Archer, Assistant Secretary, Cyber Affairs and Critical Technology Branch, Ministry of Foreign Affairs of Australia.

16 M. Rekowski et al. (eds), 'Geopolitics of emerging and disruptive technologies', The Kosciuszko Institute, 21 October 2020.

number of reported cases in which digital technologies are being used to supress human and civil rights or democracy.[17] While democratic countries strive to implement effectively regulatory measures protecting the privacy and liberties of their citizens, authoritarian regimes look for digital means to control their populations and ensure domestic stability. For example, both China and Russia have been developing measures (technological, legal and institutional) to censor online content, thwart political dissent and, if needed, separate their populations from access to the global internet.

From this second challenge stems the third: since digital technologies are being exploited by great powers for geopolitical reasons, questions about which technology provider to choose in developing digital infrastructure cease to be purely economic, but gain both political and security dimensions. The global coronavirus pandemic has fostered a new dynamic, where states more often fight over supply chains and weaponize economic interdependencies between each other.[18] Some may find themselves in a situation where the most affordable or attractive market offer comes from a provider that has links to their strategic competitors. As showcased by the recent debate on the security of 5G equipment used in national deployment plans, countries in Europe and Asia come under pressure to decide between technologies that are cheap and available but raise security concerns, or those that seem more trust-worthy but also more costly at the same time. Most countries in both Europe and Asia share their dependence on ICT products from either the United States or China, as they often lack domestic capabilities to build digital infrastructure based on home-grown technologies. For many of them, the economic dilemmas related to infrastructure development are increasingly also geopolitical.

THE POTENTIAL FOR COOPERATION

Given the shared challenges, the rationale for cooperation between Europe and Asia is therefore significant. In particular, there is a strong potential for partnerships between those countries that can be considered as like-minded in their commitment to democracy and ensuring an open, inclusive and secure digital infrastructure. This group includes – as well as the 27 EU member states – key democratic Asian powers such as Japan, India, South Korea and Singapore, and Australia, which all want to contribute to a more open, free and secure global internet governed through multi-stakeholder formats. They share similar concerns related to the deployment of digital technologies and are often targeted by threat actors of the same origin.

Examples of such alignment on digital values have already brought some of them together. Japan and India, for example, have entered a number of joint initiatives with the EU, including bilateral cyber dialogues: the EU–Japan Connectivity Partnership of 2019; and the India–EU Connectivity Partnership of 2021. In May 2022, Japan became the first country that the EU has joined with in a Digital Partnership, which aims to provide policy alignment and facilitate collaboration on a wide range of digital challenges, including supply chains, digital connectivity and digital infrastructure.[19] Japan has emerged as a global leader in digital policy,[20] with a growing portfolio of initiatives, including a 2021 Integrated Innovation Strategy, 2021 Cyber-Security Strategy and – published in June 2022 – Cyber-Security Policy for Critical Infrastructure Protection, which set out an ambitious framework for secure and resilient digital infrastructure. In April 2022, India and the EU announced the launch of a Trade and Technology Council, a political platform to develop 'deeper strategic cooperation' on 'trusted technology and security'.[21] As India is moving towards a new cyber-security strategy, momentum is building for the EU and

17 A. Polyakowa and C. Meserole, 'Exporting digital authoritarianism: the Russian and Chinese models', Brookings, August 2019.

18 Good discussions of this new international reality were recently provided by Mark Leonard, The Age of Unpeace (London: Bantam Press, 2021); and Thomas Gomart, Guerres Invisibles (Paris: Éditions Tallandier, 2021).

19 'EU–Japan summit: strengthening our partnership', European Commission, 12 May 2022.

20 L. Broeckaert, 'Digital transformation in Japan: assessing business opportunities for EU SMEs', EU–Japan Centre for Industrial Cooperation, February 2022.

21 'EU–India: joint press release on launching the Trade and Technology Council', European Commission, 25 April 2022.

India to work towards greater synergy on the security of digital infrastructure. South Korea, another emerging global leader in cyber-resilience policy, is also among the EU's closest partners in Asia.[22] The government in Seoul has been developing its policy on the protection of digital infrastructure for years and has managed to build a robust ecosystem dedicated to this task.[23] In 2019, South Korea adopted its National Cyber-Security Strategy, with securing South Korea's critical infrastructure as its primary strategic objective, as well as the National Cyber-Security Basic Plan. Today, South Korea has gathered significant experience in cyber-security governance and public–private cooperation for the protection of infrastructure that it can share with partners in the EU and elsewhere. Another emerging global leader in cyber-security policy is Singapore. Resilient infrastructure is the first pillar of its 2021 Cyber-Security Strategy and, in 2022, further ambitious measures were announced to expand and enhance protection of information infrastructure, including to virtual assets.[24] Just like South Korea, Singapore can share its tested solutions and good practices when it comes to a comprehensive governance of cyber-resilient infrastructure. Finally, Australia is another natural partner for the EU to join with in this endeavour. In 2021, Australia launched its International Cyber and Critical Technology Engagement Strategy, which underlines the importance of partnerships with international stakeholders in building trusted infrastructure for the entire Asia–Pacific region. Today, Australia remains actively engaged beyond its borders, supporting cyber-security capacity-building measures in different parts of the world and effectively leading in promotion and strengthening of cyber-security cooperation for trusted connectivity.

Another important axis for cooperation is between organizations of regional integration. The EU and the Association of South-East Asian Nations (ASEAN) have cultivated strong political and economic ties for decades, and today ASEAN is the EU's third largest trading partner outside Europe, while the EU remains the biggest investor in ASEAN countries.[25] As the EU is committed to strengthening international multilateralism, ASEAN is a natural partner also for cooperation in the digital domain. Recent examples of such cooperation include YAKSHA, a joint EU–ASEAN project aimed to develop cyber-security software solutions that gathered participants from six EU and three ASEAN member states. The EU Strategy for Cooperation in the Indo-Pacific, presented in 2021, underlines combatting cyber-crime, cyber-security capacity-building and increasing cyber resilience as the EU's aims in the region. These objectives will be pursued within a project called Enhancing Security Cooperation in and with Asia (ESIWA), which aims to deepen the security dialogue between partners in Europe and Asia. In its first stage, ESIWA engages the following partners based on their key contribution to four priority areas that include cyber security and combatting hybrid threats: India; Indonesia; Japan; South Korea; Singapore; and Vietnam. The good practices and governance experience gathered in these initiatives will provide solid ground for cooperation in developing a secure and resilient digital infrastructure, an area of joint action that is yet to be expanded to deliver tangible projects.

CRITICAL PRINCIPLES FOR THE DEVELOPMENT OF TRUSTWORTHY DIGITAL INFRASTRUCTURE

Cooperative efforts towards building secure and resilient digital infrastructure in and between Europe and Asia could start with a focus on four domains: (1) policy coordination on key values and principles; (2) joint development of standards and regulations; (3) adopting security-by-design as a guiding principle; and (4) providing economic opportunities.

22 K. Chang-beom at el. (eds), 'Korea–EU cooperation: moving to the next level', KF-VUB Korea Chair, April 2022.

23 As explained by So Jeong Kim during AESCON, South Korea has consequently been building its framework for the protection of digital infrastructure since the adoption of the Critical Information Infrastructure Protection Act in 2001, which has been regularly reviewed since. Strong commitment to the challenge of infrastructure protection, along with a broad government approach, allowed South Korea to develop a robust digital infrastructure protection ecosystem.

24 A. Leck and K. Chia, 'Singapore: new initiatives to ensure digital security and enhanced cyber resilience', Connect on Tech blog, 28 March 2022.

25 'Association of South East Asian Nations', European Commission.

First, partners in Europe and Asia should accelerate their work towards common alignment on fundamental rules for the further development and adoption of digital technologies. This relates not only to governments and political actors, but also to major stakeholders representing the security establishments, private sector, academia and civil society. The EU is already discussing track 1.5 dialogues with some Asian countries, such as South Korea, and intensifying such initiatives, as well as the proliferation of multi-stakeholder platforms for discussion and cooperation that create a feedback loop from key players beyond only the government sector, would be beneficial for greater mutual understanding and synergies. The development of digital infrastructure should be viewed as an element of more comprehensive strategies that take into account the necessary means and mechanisms to ensure the protection of core values of human and civil rights, open society and democracy. All digital projects should be considered with an acknowledgment of current and future technology capabilities, their potential uses and their impact on the protection of fundamental rights. As our world is increasingly being transformed by both the digital revolution and geopolitical competition, technology and digital infrastructure cannot be dissociated from concerns about safeguarding key values of our societies.

Second, a common understanding of policy fundamentals should lead to cooperation on regulations, certification and the development of standards for digital infrastructure. Standardization and regulation play an important role in ensuring secure and resilient digital connectivity,[26] as they contribute to the establishment of an environment that favours sustainability, transparency, openness, interoperability and trustworthiness. Shared agreements on standards and regulatory rationales on the political level would make it easier for public and private partners to get together and produce joint projects, as this would establish a clear set of rules to follow and a better-defined pool of resources (such as certified equipment vendors or security products) from which to draw. This should be based on the cyber-security frameworks mentioned in the previous paragraph, as well as the EU's rapidly developing portfolio. The standards and measures that constitute the EU cyber-security fabric already include the Cyber-Security Strategy, Cyber-Security Act, the revised Network and Information Security Directive, 5G Toolbox, Data Governance Act, the upcoming Cyber Resilience Act and the General Data Protection Regulation. What is more, partners in Asia and Europe could benefit from the establishment of a global digital resilience agreement that would focus on standards for digital connectivity.[27] They should work towards greater harmonization and convergence on such standards, which should also include sustainability.[28]

Third, all joint digital infrastructure projects should first and foremost focus on embedding security-by-design as a guiding principle. This could be implemented as a requirement – for example, by the EU and its Asian partners – for any future international infrastructure projects developed with joint funding. The planning and design of projects should already consider cyber security and integrity at every stage of the infrastructure life cycle, from development to management to risk mitigation in the end stages such as decommissioning.[29] It is also paramount to underline the necessity to secure the ICT components that underpin other functional infrastructures, such as transport, energy, or other critical utilities. Future infrastructure-building efforts should be supplemented by endeavours to share and exchange knowledge and good practices on the identification and mitigation of risks related to the digital infrastructure development process.

26 The crucial importance of greater cooperation between Europe and Asia–Pacific on standardization was highlighted by all of the speakers during the panel at AESCON.

27 This idea was suggested by Patryk Pawlak (Executive Officer, Brussels Bureau, European Union Institute for Security Studies) during AESCON.

28 During the discussion at AESCON, Hilary Mine (Vice President for Strategy & Technology, CX at Nokia) defined responsible infrastructure as one that maximizes the positive environmental and social impact on the world – the handprint – while minimizing the negative impact – the footprint.

29 The critical importance of addressing the entire life cycle of digital products with security requirements was particularly stressed during the panel at AESCON by Hilary Mine.

Finally, the creation of economically viable opportunities to enable access to secure and cost-effective technologies that adhere to transparency, scrutiny and responsible management is crucial. New financial mechanisms that would allow less-wealthy states to acquire equipment and services from trustworthy vendors – and not only the most affordable – should be put in place. For the developing countries, the need to choose between cheap or secure should be eliminated. The security of components and services in the supply chains is a central requirement, not only for ensuring resilient connectivity for the end-users, but for building a stable environment for social and economic development in general. The EU is willing to cooperate and support infrastructure development with foreign partners under its Global Gateway scheme, which promises €300 billion of investments, including in the digital sector and with security as one of the six key principles. Partners in Asia and Europe should work together to establish access to technologies that are both affordable and verified, thus increasing the chances of their adoption by less-wealthy countries in both regions. Such initiatives should also focus on increasing the diversity of available technologies to limit the dependence on single technology providers. Maintaining open, competitive and diverse technology markets is crucial for ensuring states' and societies' digital sovereignty and freedom to define their own technological development.[30] Moreover, to overcome the dependence on foreign technologies that is generally common in many European and Asian countries, far-sighted and strategically planned investment in research-and-development (R&D) activities is required. Being scientific powerhouses of the world, partners in Europe and Asia should work closer together on the development of novel technologies that will build up their digital sovereignty. For example, jointly with the governments of its closest Asian partners, the EU could co-create a framework providing funds for inter-regional R&D projects in key emerging technologies. In this way, both regions would also strengthen their positions in the global value chain.

Series editors: Maaike Okano-Heijmans and Brigitte Dekker[31]

30 As pointed out by Cameron Archer during the discussion at AESCON, secure and cost-effective technologies are also dependent on market choice.

31 The author wishes to acknowledge valuable feedback from the reviewers of an earlier version of this paper, in particular AESCON panellist So Jeong Kim, Senior Research Fellow at the Institute for National Security Strategy, South Korea.

Michał Rekowski

SECURE AND RESILIENT DIGITAL INFRASTRUCTURE: AN AGENDA FOR EUROPE AND ASIA

AESCON Policy Brief 02-2022 | July

ABOUT THE AUTHOR

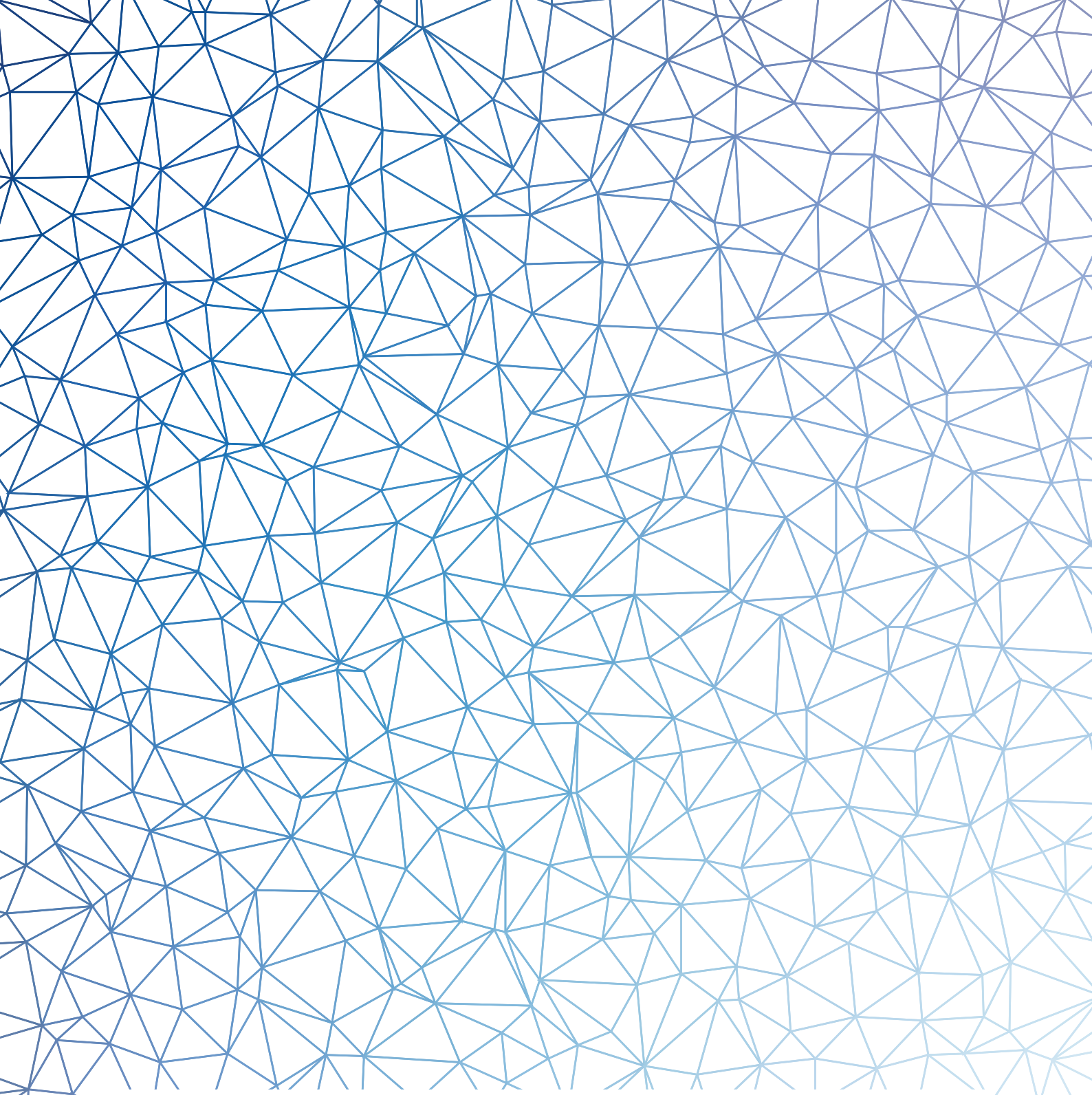
Michał Rekowski is a researcher working on the politics of cyber security and emerging technologies, as well as the EU digital, security and defence policies. He is the Principal Investigator for a multi-annual research project on European Strategic Autonomy, financed by the National Science Centre, Poland. From 2020 to 2022, he was Programme Director of the European Cyber Security Forum: CYBERSEC.

ABOUT THE AESCON POLICY BRIEF SERIES

This Policy Brief is one of a series that sprang from the Asia–Europe Sustainable Connectivity (AESCON) conference held from 22–24 March 2022. The five Policy Briefs present the main findings and policy recommendations from the various AESCON panels.

The series is edited by Maaike Okano-Heijmans and Brigitte Dekker of the Clingendael Institute, and includes the following pieces:

- *Multistakeholderism: the path to human-centred digital connectivity, by Maaike Okano-Heijmans and Vanshika Shah of the Clingendael Institute, The Hague*
- *Secure and resilient digital infrastructure: an agenda for Europe and Asia, by Michał Rekowski of the Kosciuszko Institute, Kraków*
- *Putting trust back in trusted connectivity: a call for more congruence in cross-border data transfers, by Priyadarshini D of Carnegie India, New Delhi*
- *Digital connectivity and opportunities for development cooperation between Asia and Europe, by Christina Stansell, Fabian Hohmann and Elisabeth Gager of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Bonn*
- *Linking digital trajectories: Asia and Europe's opportunities in the digital economy, by Karthik Nachiappan of the Institute of South Asian Studies, Singapore*



Asia-Europe Meeting

Clingendael
Netherlands Institute of International Relations

Funded by
the European Union

CARNEGIE
INDIA

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

NUS National University of Singapore | ISAS Institute of South Asian Studies

The Kosciuszko Institute